



STATE OF OKLAHOMA CONTRACT WITH AUTOMOATED HEALTH SYSTEMS, INC.

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 (“State”) and Automated Health Systems, Inc. (“Supplier”) and is effective as of the effective date set forth on a properly issued purchase order or, if no effective date is listed, the date of last signature (“Effective Date”).

Purpose

The State is awarding the Contract to Supplier for the provision of purchasing Call/Contact Center Staffing and Management services for various State agencies, as more particularly described in certain Contract documents. The Supplier requested no exceptions and no additional terms. This Contract document memorializes the agreement of the parties with respect to terms of the Contract that is being awarded to Supplier.

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

1. The parties agree that Supplier has not yet begun performance of work under the Contract. Upon full execution of the 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, Attachment A;
 - 2.2. General Terms, Attachment B;
 - 2.3. Statewide Terms, Attachment C;
 - 2.4. Information Technology Terms, Attachment D;
 - 2.5. Price, Attachment E-1
 - 2.6. Response to Specification, Attachment E-2
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. The State agrees to maintain the Security Certification and Accreditation Assessment found in Supplier’s bid as confidential. No other information requested to be held confidential was deemed confidential by the State.

- 3.2. Supplier provided a value add option in their bid response. The State declines the value add.
 - 3.3. To the extent any term or condition in any Contract Document, including via a hyperlink or uniform resource locator, conflicts with an applicable Oklahoma and/or United States law or regulation, such term or condition is void and unenforceable. By executing any Contract Document which contains a conflicting term or condition, the State or Customer makes no representation or warranty regarding the enforceability of such term or condition and the State or Customer does not waive the applicable Oklahoma and/or United States law or regulation which conflicts with the term or condition.
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

AUTOMATED HEALTH SYSTEMS, INC.

By: *Amanda Otis*
Amanda Otis (May 30, 2024 08:18 CDT)

Name: Amanda Otis

Title: State Purchasing Director

Date: May 30, 2024

By: 

Name: Joseph P Cain III, CPA

Title: Chief Financial Officer

Date: 5/28/24

ATTACHMENT A
SOLICITATION NO. 0900000546

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 (OMES) Information Services Division (ISD) 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 for a Call/Contact Center Staffing and Management services for various State agencies. OMES's mission is to enhance Oklahoma's citizen experience in responsive communications by having a dedicated Call/Contact Center that is managed as a complete solution.

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 four (4) one-year options to renew the Contract.

2. Scope of Work

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

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

Certain Contract requirements and terms are set forth below as Exhibit 3.

Certain Contract requirements and terms are set as Exhibit 4 – Pricing.

EXHIBIT 1

- I. The Supplier must provide the staffing, consulting, and management as determined by the Customers procuring services based on their specific business needs. When a need is identified, a Statement of Work with Customer specific business requirements and technical specifications will be created by the Customer and sent to the Supplier. Business specific requirements will address operational workflows, detailed system interface requirements, a customization/configuration traceability component and provide for the testing and documented results required by each Customer.
- II. This Contract will provide Call/Contact Center services with world-class support for various Customers. These services include but are not limited to:
 1. Inbound and Outbound Live Operator Services
 2. Service or Product Information
 3. Scripted Information Dissemination
 4. Data Entry of Application/Form Information into State or Contractor Database
 5. Mailing and Fulfillment Services
 6. Bilingual Service – Spanish/English/
 7. Voice Mail
 8. Automatic Call Distributor (ACD)
 9. Interactive Voice Response (IVR)
 10. Email Correspondence
 11. Call Center Overflow Capabilities
 12. Handling Surveys & Questionnaires
 13. Managed Services in which hardware and software are dedicated to a particular customer and run on that customer's premises or third-party data center but are managed by a third-party service provider.
- III. Customer Responsibilities
 1. The Customer will provide the initial training documentation and ongoing support from the subject matter experts.
 2. The Customer will provide secure access to the Nice CXOne statewide platform.
 3. The Customer will provide secure remote access to all required Customer Service Systems.

Exhibit 2 – IRS Publication 1075
Safeguarding Contract Language for General Services

I. PERFORMANCE

In performance of this contract, the Contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

- (1) All work will be performed under the supervision of the contractor or the contractor's responsible employees.
- (2) The contractor and the contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.
- (3) Any Federal tax returns or return information (hereafter referred to as returns or return information) made available shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone other than an officer or employee of the contractor is prohibited.
- (4) All returns and return information will be accounted for upon receipt and properly stored before, during and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.
- (5) No work involving returns and return information furnished under this contract will be subcontracted without prior written approval of the IRS.
- (6) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.
- (7) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

(Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS

Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as five years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized future disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.

- (1) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000.00 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of \$1,000.00 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. The penalties are prescribed by IRCs 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.
- (2) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.
- (3) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of [IRCs 7431, 7213 and 7213A](#) in [IRS Publication 1075](#). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 1.8, Reporting Improper Inspections or Disclosures in [IRS Publication 1045](#).) For both the initial certification and the annual certification, the contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. DATA INCIDENT RESPONSE

The contractor will:

- (1) Cooperate with and exchange information with agency officials, as determined necessary by the agency, in order to effectively report and manage a suspected or confirmed breach.
- (2) Properly encrypt FTI in accordance with Publication 1075 and other applicable policies and to comply with any agency-specific policies for protecting FTI.
- (3) Complete regular training on how to identify and report a breach;
- (4) Report a suspected or confirmed breach in any medium or form, including paper, oral and electronic, as soon as possible and without unreasonable delay, consistent with the agency's incident management policy;
- (5) Maintain capabilities to determine what FTI was or could have been accessed and by whom, construct a timeline of user activity, determine methods and techniques used to access FTI and identify the initial attack vector; Allow for an inspection, investigation, forensic analysis and any other action necessary to ensure compliance with Publication 1075, the agency's breach response plan and to assist with responding to a breach; Identify roles and responsibilities, in accordance with Publication 1075 and the agency's breach response plan; and, explain that a report of a breach shall not, by itself, be interpreted as evidence that the contractor or its subcontractor failed to provide adequate safeguards for FTI.

IV. INSPECTION

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

Exhibit 3 – IRS Publication 1075
Safeguarding Contract Language for Technology Services

I. PERFORMANCE

In performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

- (1) All work will be done under the supervision of the contractor or the contractor's employees.
- (2) The contractor and the contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.
- (3) Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the contractor will be prohibited.
- (4) All returns and return information will be accounted for upon receipt and properly stored before, during and after processing. In addition, all related output will be given the same level of protection as required for the source material.
- (5) The contractor certifies that the data processed during the performance of this contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.
- (6) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.
- (7) All computer systems receiving, processing, storing, accessing, protecting and/or transmitting FTI must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational and technical controls. All security features must be available and activated to protect against unauthorized use of and access to Federal Tax Information.
- (8) No work involving Federal Tax Information furnished under this contract will be subcontracted without prior written approval of the IRS.

- (9) The contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.
- (10) The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

(Include any additional safeguards that may be appropriate.)

II. CRIMINAL/CIVIL SANCTIONS

- (1) Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.
- (2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of \$1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.
- (3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that

disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

- (4) Granting a contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, contractors must be advised of the provisions of [IRCs 7431, 7213 and 7213A](#) in [IRS Publication 1075](#). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 1.8, Reporting Improper Inspections or Disclosures in [IRS Publication 1045](#).) For both the initial certification and the annual certification, the contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. DATA INCIDENT RESPONSE

The contractor will:

- (1) Cooperate with and exchange information with agency officials, as determined necessary by the agency, in order to effectively report and manage a suspected or confirmed breach.
- (2) Properly encrypt FTI in accordance with Publication 1075 and other applicable policies and to comply with any agency-specific policies for protecting FTI.
- (3) Complete regular training on how to identify and report a breach;
- (4) Report a suspected or confirmed breach in any medium or form, including paper, oral and electronic, as soon as possible and without unreasonable delay, consistent with the agency's incident management policy;
- (5) Maintain capabilities to determine what FTI was or could have been accessed and by whom, construct a timeline of user activity, determine methods and techniques used to access FTI and identify the initial attack vector; Allow for an inspection, investigation, forensic analysis and any other action necessary to ensure compliance with Publication 1075, the agency's breach response plan and to assist with responding to a breach; Identify roles and responsibilities, in accordance with Publication 1075 and the agency's breach response plan; and, explain that a report of a breach shall not, by itself, be interpreted as evidence that the contractor or its subcontractor failed to provide adequate safeguards for FTI.

IV. INSPECTION

The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The

IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. On the basis of such inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with contract safeguards.

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 debaring 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 (viii) all Intellectual Property Rights in any of the foregoing, and which are or were created,

prepared, developed, invented or conceived for the use of benefit of Customer in connection with this Contract or with funds appropriated by or for Customer or Customer's benefit (a) by any Supplier personnel or Customer personnel or (b) any Customer personnel who then became personnel to Supplier or any of its affiliates or subcontractors, where, although creation or reduction-to-practice is completed while the person is affiliated with Supplier or its personnel, any portion of same was created, invented or conceived by such person while affiliated with Customer.

5 Pricing

- 5.1** Pursuant to 68 O.S. §§ 1352, 1356, and 1404, State agencies are exempt from the assessment of State sales, use, and excise taxes. Further, State agencies and political subdivisions of the State are exempt from Federal Excise Taxes pursuant to Title 26 of the United States Code. Any taxes of any nature whatsoever payable by the Supplier shall not be reimbursed.
- 5.2** Pursuant to 74 O.S. §85.40, all travel expenses of Supplier must be included in the total Acquisition price.
- 5.3** The price of a product offered under the Contract shall include and Supplier shall prepay all shipping, packaging, delivery and handling fees. All product deliveries will be free on board Customer's Destination. No additional fees shall be charged by Supplier for standard shipping and handling. If Customer requests expedited or special delivery, Customer may be responsible for any charges for expedited or special delivery.

6 Ordering, Inspection, and Acceptance

- 6.1** Any product or service furnished under the Contract shall be ordered by issuance of a valid purchase order or other appropriate payment mechanism, including a pre-encumbrance, or by use of a valid Purchase Card. All orders and transactions are governed by the terms and conditions of the Contract. Any purchase order or other applicable payment mechanism dated prior to termination or expiration of the Contract shall be performed unless mutually agreed in writing otherwise.
- 6.2** Services will be performed in accordance with industry best practices and are subject to acceptance by the Customer. Notwithstanding any other provision in the Contract, deemed acceptance of a service or associated deliverable shall not apply automatically upon receipt of a deliverable or upon provision of a service.

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

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

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

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

7 Invoices and Payment

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

The following terms additionally apply:

- A.** An invoice shall contain the purchase order number, description of products or services provided and the dates of such provision.
- B.** Failure to provide a timely and proper invoice may result in delay of processing the invoice for payment. Proper invoice is defined at OAC 260:10-1-2.
- C.** Payment of all fees under the Contract shall be due NET 45 days. Payment and interest on late payments are governed by 62 O.S. §34.72. Such interest is the sole and exclusive remedy for late payments by a State agency and no other late fees are authorized to be assessed pursuant to Oklahoma law.
- D.** The date from which an applicable early payment discount time is calculated shall be from the receipt date of a proper invoice. There is no obligation, however, to utilize an early payment discount.
- E.** If an overpayment or underpayment has been made to Supplier any subsequent payments to Supplier under the Contract may be adjusted to correct the account. A written explanation of the adjustment will be issued to Supplier.
- F.** Supplier shall have no right of setoff.
- G.** Because funds are typically dedicated to a particular fiscal year, an invoice will be paid only when timely submitted, which shall in no instance be later than six (6) months after the end of the fiscal year in which the goods are provided or services performed.
- H.** The Supplier shall accept payment by Purchase Card as allowed by Oklahoma law.

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

8.1 As a condition of this Contract, Supplier shall procure at its own expense, and provide proof of, insurance coverage with the applicable liability limits set

forth below and any approved subcontractor of Supplier shall procure and provide proof of the same coverage. The required insurance shall be underwritten by an insurance carrier with an A.M. Best rating of A- or better.

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

- A.** Workers' Compensation and Employer's Liability Insurance in accordance with and to the extent required by applicable law;
- B.** Commercial General Liability Insurance covering the risks of personal injury, bodily injury (including death) and property damage, including coverage for contractual liability, with a limit of liability of not less than \$5,000,000 per occurrence;
- C.** Automobile Liability Insurance with limits of liability of not less than \$5,000,000 combined single limit each accident;
- D.** Directors and Officers Insurance which shall include Employment Practices Liability as well as Consultant's Computer Errors and Omissions Coverage, if information technology services are provided under the Contract, with limits not less than \$5,000,000 per occurrence;
- E.** Security and Privacy Liability insurance, including coverage for failure to protect confidential information and failure of the security of Supplier's computer systems that results in unauthorized access to Customer data with limits \$5,000,000 per occurrence; and
- F.** Additional coverage required in writing in connection with a particular Acquisition.

- 8.2** Supplier shall be entirely responsible during the existence of the Contract for the liability and payment of taxes payable by or assessed to Supplier or its employees, agents and subcontractors of whatever kind, in connection with the Contract. Supplier further agrees to comply with all state and federal laws applicable to any such persons, including laws regarding wages, taxes, insurance, and Workers' Compensation. Neither Customer nor the State shall be liable to the Supplier, its employees, agents, or others for the payment of taxes or the provision of unemployment insurance and/or Workers' Compensation or any benefit available to a State or Customer employee.
- 8.3** Supplier agrees to indemnify Customer, the State, and its employees, agents, representatives, contractors, and assignees for any and all liability, actions, claims, demands, or suits, and all related costs and expenses (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) relating to tax liability, unemployment insurance and/or Workers' Compensation in connection with its performance under the Contract.

9 Compliance with Applicable Laws

- 9.1** As long as Supplier has an obligation under the terms of the Contract and in connection with performance of its obligations, the Supplier represents its present compliance, and shall have an ongoing obligation to comply, with all applicable federal, State, and local laws, rules, regulations, ordinances, and orders, as amended, including but not limited to the following:
- A.** Drug-Free Workplace Act of 1988 set forth at 41 U.S.C. §81.
 - B.** Section 306 of the Clean Air Act, Section 508 of the Clean Water Act, Executive Order 11738, and Environmental Protection Agency Regulations which prohibit the use of facilities included on the EPA List of Violating Facilities under nonexempt federal contracts, grants or loans;
 - C.** Prospective participant requirements set at 45 C.F.R. part 76 in connection with Debarment, Suspension and other responsibility matters;
 - D.** 1964 Civil Rights Act, Title IX of the Education Amendment of 1972, Section 504 of the Rehabilitation Act of 1973, Americans with Disabilities Act of 1990, and Executive Orders 11246 and 11375;
 - E.** Anti-Lobbying Law set forth at 31 U.S.C. §1325 and as implemented at 45 C.F.R. part 93;

- F. Requirements of Internal Revenue Service Publication 1075 regarding use, access and disclosure of Federal Tax Information (as defined therein);
 - G. Obtaining certified independent audits conducted in accordance with Government Auditing Standards and Office of Management and Budget Uniform Guidance, 2 CFR 200 Subpart F §200.500 et seq. with approval and work paper examination rights of the applicable procuring entity;
 - H. Requirements of the Oklahoma Taxpayer and Citizen Protection Act of 2007, 25 O.S. §1312 and applicable federal immigration laws and regulations and be registered and participate in the Status Verification System. The Status Verification System is defined at 25 O.S. §1312, includes but is not limited to the free Employment Verification Program (E-Verify) through the Department of Homeland Security, and is available at www.dhs.gov/E-Verify;
 - I. Requirements of the Health Insurance Portability and Accountability Act of 1996; Health Information Technology for Economic and Clinical Health Act; Payment Card Industry Security Standards; Criminal Justice Information System Security Policy and Security Addendum; and Family Educational Rights and Privacy Act; and
 - J. Be registered as a business entity licensed to do business in the State, have obtained a sales tax permit, and be current on franchise tax payments to the State, as applicable.
- 9.2 The Supplier's employees, agents and subcontractors shall adhere to applicable Customer policies including, but not limited to acceptable use of Internet and electronic mail, facility and data security, press releases, and public relations. As applicable, the Supplier shall adhere to the [State Information Security Policy, Procedures, Guidelines](#). Supplier is responsible for reviewing and relaying such policies covering the above to the Supplier's employees, agents and subcontractors.
- 9.3 At no additional cost to Customer, the Supplier shall maintain all applicable licenses and permits required in association with its obligations under the Contract.
- 9.4 In addition to compliance under subsection 9.1 above, Supplier shall have a continuing obligation to comply with applicable Customer-specific mandatory contract provisions required in connection with the receipt of federal funds or other funding source.

- 9.5** The Supplier is responsible to review and inform its employees, agents, and subcontractors who provide a product or perform a service under the Contract of the Supplier's obligations under the Contract and Supplier certifies that its employees and each such subcontractor shall comply with minimum requirements and applicable provisions of the Contract. At the request of the State, Supplier shall promptly provide adequate evidence that such persons are its employees, agents or approved subcontractors and have been informed of their obligations under the Contract.
- 9.6** As applicable, Supplier agrees to comply with the Governor's Executive Orders related to the use of any tobacco product, electronic cigarette or vaping device on any and all properties owned, leased, or contracted for use by the State, including but not limited to all buildings, land and vehicles owned, leased, or contracted for use by agencies or instrumentalities of the State.
- 9.7** The execution, delivery and performance of the Contract and any ancillary documents by Supplier will not, to the best of Supplier's knowledge, violate, conflict with, or result in a breach of any provision of, or constitute a default (or an event which, with notice or lapse of time or both, would constitute a default) under, or result in the termination of, any written contract or other instrument between Supplier and any third party.
- 9.8** Supplier represents that it has the ability to pay its debts when due and it does not anticipate the filing of a voluntary or involuntary bankruptcy petition or appointment of a receiver, liquidator or trustee.
- 9.9** Supplier represents that, to the best of its knowledge, any litigation or claim or any threat thereof involving Supplier has been disclosed in writing to the State and Supplier is not aware of any other litigation, claim or threat thereof.
- 9.10** If services provided by Supplier include delivery of an electronic communication, Supplier shall ensure such communication and any associated support documents are compliant with Section 508 of the Federal Rehabilitation Act and with State standards regarding accessibility. Should any communication or associated support documents be non-compliant, Supplier shall correct and re-deliver such communication immediately upon discovery or notice, at no additional cost to the State. Additionally, as part of compliance with accessibility requirements where documents are only provided in non-electronic format, Supplier shall promptly provide such communication and any associated support documents in an alternate format usable by individuals with disabilities upon request and at no additional cost, which may originate from an intended recipient or from the State.

10 Audits and Records Clause

- 10.1** As used in this clause and pursuant to 67 O.S. §203, “record” includes a document, book, paper, photograph, microfilm, computer tape, disk, record, sound recording, film recording, video record, accounting procedures and practices, and other data, regardless of type and regardless of whether such items are in written form, in the form of computer data, or in any other form. Supplier agrees any pertinent federal or State agency or governing entity of a Customer shall have the right to examine and audit, at no additional cost to a Customer, all records relevant to the execution and performance of the Contract except, unless otherwise agreed, costs of Supplier that comprise pricing under the Contract.
- 10.2** The Supplier is required to retain records relative to the Contract for the duration of the Contract and for a period of seven (7) years following completion or termination of an Acquisition unless otherwise indicated in the Contract terms. If a claim, audit, litigation or other action involving such records is started before the end of the seven-year period, the records are required to be maintained for two (2) years from the date that all issues arising out of the action are resolved, or until the end of the seven (7) year retention period, whichever is later.
- 10.3** Pursuant to 74 O.S. §85.41, if professional services are provided hereunder, all items of the Supplier that relate to the professional services are subject to examination by the State agency, State Auditor and Inspector and the State Purchasing Director.

11 Confidentiality

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

services under the Contract. The Supplier further warrants that it has a tested and proven system in effect designed to protect all confidential information.

- 11.2** Supplier shall establish, maintain and enforce agreements with all such persons and entities that have access to State and citizen data and records to fulfill Supplier's duties and obligations under the Contract and to specifically prohibit any sale, assignment, conveyance, provision, release, dissemination or other disclosure of any State or citizen data or records except as required by law or allowed by written prior approval of the Customer.
- 11.3** Supplier shall immediately report to the Customer any and all unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of any State or citizen data or records of which it or its parent company, subsidiaries, affiliates, employees, officers, directors, assignees, agents, representatives, independent contractors, and subcontractors is aware or have knowledge or reasonable should have knowledge. The Supplier shall also promptly furnish to Customer full details of the unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination, or attempt thereof, and use its best efforts to assist the Customer in investigating or preventing the reoccurrence of such event in the future. The Supplier shall cooperate with the Customer in connection with any litigation and investigation deemed necessary by the Customer to protect any State or citizen data and records and shall bear all costs associated with the investigation, response and recovery in connection with any breach of State or citizen data or records including but not limited to credit monitoring services with a term of at least three (3) years, all notice-related costs and toll free telephone call center services.
- 11.4** Supplier further agrees to promptly prevent a reoccurrence of any unauthorized use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of State or citizen data and records.
- 11.5** Supplier acknowledges that any improper use, appropriation, sale, assignment, conveyance, provision, release, access, acquisition, disclosure or other dissemination of any State data or records to others may cause immediate and irreparable harm to the Customer and certain beneficiaries and may violate state or federal laws and regulations. If the Supplier or its affiliates, parent company, subsidiaries, employees, officers, directors, assignees, agents, representatives, independent contractors, and subcontractors improperly use, appropriate, sell, assign, convey, provide, release, access, acquire, disclose or otherwise disseminate such confidential information to any person or entity in

violation of the Contract, the Customer will immediately be entitled to injunctive relief and/or any other rights or remedies available under this Contract, at equity or pursuant to applicable statutory, regulatory, and common law without a cure period.

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

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

12 Conflict of Interest

In addition to any requirement of law or of a professional code of ethics or conduct, the Supplier, its employees, agents and subcontractors are required to disclose any outside activity or interest that conflicts or may conflict with the best interest of the State. Prompt disclosure is required under this section if the activity or interest is related, directly or indirectly, to any person or entity currently under contract with or seeking to do business with the State, its employees or any other third-party individual or entity awarded a contract with the State. Further, as long as the Supplier has an

obligation under the Contract, any plan, preparation or engagement in any such activity or interest shall not occur without prior written approval of the State. Any conflict of interest shall, at the sole discretion of the State, be grounds for partial or whole termination of the Contract.

13 Assignment and Permitted Subcontractors

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

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

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

obtaining prior written approval by the State of any subcontractor and associated employees shall be a continuing obligation. The State further reserves the right to revoke approval of a subcontractor or an employee thereof in instances of poor performance, misconduct or for other similar reasons.

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

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

14 Background Checks and Criminal History Investigations

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

15 Patents and Copyrights

Without exception, a product or deliverable price shall include all royalties or costs owed by the Supplier to any third party arising from the use of a patent, intellectual property, copyright or other property right held by such third party. Should any third party threaten or make a claim that any portion of a product or service provided by Supplier under the Contract infringes that party's patent, intellectual property, copyright or other property right, Supplier shall enable each affected Customer to legally continue to use, or modify for use, the portion of the product or service at issue or replace such potentially infringing product, or re-perform or redeliver in the case of

a service, with at least a functional non-infringing equivalent. Supplier's duty under this section shall extend to include any other product or service rendered materially unusable as intended due to replacement or modification of the product or service at issue. If the Supplier determines that none of these alternatives are reasonably available, the State shall return such portion of the product or deliverable at issue to the Supplier, upon written request, in exchange for a refund of the price paid for such returned goods as well as a refund or reimbursement, if applicable, of the cost of any other product or deliverable rendered materially unusable as intended due to removal of the portion of product or deliverable at issue. Any remedy provided under this section is not an exclusive remedy and is not intended to operate as a waiver of legal or equitable remedies because of acceptance of relief provided by Supplier.

16 Indemnification

16.1 Acts or Omissions

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

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

16.2 Infringement

Supplier shall indemnify the Indemnified Parties, as applicable, for all liability, claims, damages, losses, costs, expenses, demands, suits and actions of third parties (including without limitation reasonable attorneys' fees and costs required to establish the right to indemnification) arising from or in connection

with Supplier's breach of its representations and warranties in the Contract or alleged infringement of any patent, intellectual property, copyright or other property right in connection with a product or service provided under the Contract. Supplier's duty under this section is reduced to the extent a claimed infringement results from: (a) a Customer's or user's content; (b) modifications by Customer or third party to a product delivered under the Contract or combinations of the product with any non-Supplier-provided services or products unless Supplier recommended or participated in such modification or combination; (c) use of a product or service by Customer in violation of the Contract unless done so at the direction of Supplier, or (d) a non-Supplier product that has not been provided to the State by, through or on behalf of Supplier as opposed to its combination with products Supplier provides to or develops for the State or a Customer as a system.

16.3 Notice and Cooperation

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

16.4 Coordination of Defense

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

16.5 Limitation of Liability

- A.** With respect to any claim or cause of action arising under or related to the Contract, neither the State nor any Customer shall be liable to Supplier for lost profits, lost sales or business expenditures, investments, or commitments in connection with any business, loss of any goodwill, or for any other indirect, incidental, punitive, special or consequential damages, even if advised of the possibility of such damages.
- B.** Notwithstanding anything to the contrary in the Contract, no provision shall limit damages, expenses, costs, actions, claims, and liabilities arising from or related to property damage, bodily injury or death caused by Supplier or its employees, agents or subcontractors; indemnity, security or confidentiality obligations under the Contract; the bad faith, negligence, intentional misconduct or other acts for which applicable law does not allow exemption from liability of Supplier or its employees, agents or subcontractors.
- C.** The limitation of liability and disclaimers set forth in the Contract will apply regardless of whether Customer has accepted a product or service. The parties agree that Supplier has set its fees and entered into the Contract in reliance on the disclaimers and limitations set forth herein, that the same reflect an allocation of risk between the parties and form an essential basis of the bargain between the parties. These limitations shall apply notwithstanding any failure of essential purpose of any limited remedy.

17 Termination for Funding Insufficiency

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

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

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

18 Termination for Cause

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

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

18.3 Upon receipt of notice of a termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the

termination does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Such termination is not an exclusive remedy but is in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contract or certain obligations are terminated shall be refunded. Termination of the Contract under this section, in whole or in part, shall not relieve the Supplier of liability for claims arising under the Contract.

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

19 Termination for Convenience

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

19.2 Upon receipt of notice of such termination, Supplier shall immediately comply with the notice terms and take all necessary steps to minimize the incurrence of costs allocable to the work affected by the notice. If a purchase order or other payment mechanism has been issued and a product or service has been accepted as satisfactory prior to the effective date of termination, the termination does not relieve an obligation to pay for the product or service but there shall not be any liability for further payments ordinarily due under the Contract or for any damages or other amounts caused by or associated with such termination. Such termination shall not be an exclusive remedy but shall

be in addition to any other rights and remedies provided for by law. Any amount paid to Supplier in the form of prepaid fees that are unused when the Contract or certain obligations are terminated shall be refunded. Termination of the Contract under this section, in whole or in part, shall not relieve the Supplier of liability for claims arising under the Contract.

20 Suspension of Supplier

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

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

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

21 Certification Regarding Debarment, Suspension, and Other Responsibility Matters

The certification made by Supplier with respect to Debarment, Suspension, certain indictments, convictions, civil judgments and terminated public contracts is a material representation of fact upon which reliance was placed when entering into the Contract. A determination that Supplier knowingly rendered an erroneous certification, in addition to other available remedies, may result in whole or partial termination of the Contract for Supplier's default. Additionally, Supplier shall promptly provide written

notice to the State Purchasing Director if the certification becomes erroneous due to changed circumstances.

22 Certification Regarding State Employees Prohibition From Fulfilling Services

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

23 Force Majeure

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

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

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

confidentiality, indemnification, data security or breach notification obligations set forth herein.

24 Security of Property and Personnel

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

25 Notices

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

If sent to the State:

State Purchasing Director
2401 N. Lincoln Blvd., Suite 118
Oklahoma City, Oklahoma 73105

With a copy, which shall not constitute notice, to:

Purchasing Division Deputy General Counsel
2401 N. Lincoln Blvd., Suite 118
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 118
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 (viii) 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/services/information-services/accessibility-standards>. 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://oklahoma.gov/content/dam/ok/en/omes/documents/InfoSecPPG.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.

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

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

7 Emerging Technologies

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

8 Extension Right

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

9 Source Code Escrow

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

- 9.1** A bona fide material default of the obligations of the Supplier under the agreement with the applicable Customer;
- 9.2** An assignment by the Supplier for the benefit of its creditors;
- 9.3** A failure by the Supplier to pay, or an admission by the Supplier of its inability to pay, its debts as they mature;
- 9.4** The filing of a petition in bankruptcy by or against the Supplier when such petition is not dismissed within sixty (60) days of the filing date;
- 9.5** The appointment of a receiver, liquidator or trustee appointed for any substantial part of the Supplier's property;
- 9.6** The inability or unwillingness of the Supplier to provide the maintenance and support services in accordance with the agreement with the agency;
- 9.7** Supplier's ceasing of maintenance and support of the software; or
- 9.8** Such other condition as may be statutorily imposed by the future amendment or enactment of applicable Oklahoma law.

10 Commercial Off The Shelf Software

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

11 Ownership Rights

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

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

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

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

If any Acquisition pursuant to this Contract is funded wholly or in part with federal funds, the source code and all associated software and related documentation owned by the State may be

shared with other publicly funded agencies at the discretion of the State without permission from or additional compensation to the Supplier.

12 Intellectual Property Ownership

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

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

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

prosecution of all such applications and in any legal actions and proceedings concerning the Work Product.

- 12.3** Supplier hereby irrevocably and forever waives, and agrees never to assert, any Moral Rights in or to the Work Product which Supplier may now have or which may accrue to Supplier's benefit under U.S. or foreign copyright or other laws and any and all other residual rights and benefits which arise under any other applicable law now in force or hereafter enacted. Supplier acknowledges the receipt of equitable compensation for its assignment and waiver of such Moral Rights.
- 12.4** All documents, information and materials forwarded to Supplier by Customer for use in and preparation of the Work Product shall be deemed the confidential information of Customer, subject to the license granted by Customer to Supplier hereunder. Supplier shall not otherwise use, disclose, or permit any third party to use or obtain the Work Product, or any portion thereof, in any manner without the prior written approval of Customer.
- 12.5** These provisions are intended to protect Customer's proprietary rights pertaining to the Work Product and the Intellectual Property Rights therein and any misuse of such rights would cause substantial and irreparable harm to Customer's business. Therefore, Supplier acknowledges and stipulates that a court of competent jurisdiction may immediately enjoin a material breach of the Supplier's obligations with respect to confidentiality provisions of the Contract and the Work Product and a Customer's Intellectual Property Rights, upon a request by Customer, without requiring proof of irreparable injury, as same is presumed.
- 12.6** Upon the request of Customer, but in any event upon termination or expiration of this Contract or a statement of work, Supplier shall surrender to Customer all documents and things pertaining to the Work Product, generated or developed by Supplier or furnished by Customer to Supplier, including all materials embodying the Work Product, any Customer confidential information and Intellectual Property Rights in such Work Product, regardless of whether complete or incomplete. This section is intended to apply to all Work Product as well as to all documents and things furnished to Supplier by Customer or by anyone else that pertains to the Work Product.
- 12.7** Customer hereby grants to Supplier a non-transferable, non-exclusive, royalty-free, fully paid license to use any Work Product solely as necessary to provide services to Customer. Except as provided in this section, neither Supplier nor any subcontractor shall have the right to use the Work Product in connection with the provision of services to its other customers without the prior written consent of Customer, which consent may be withheld in Customer's sole discretion.
- 12.8** To the extent that any Third Party Intellectual Property is embodied or reflected in the Work Product or is necessary to provide services, Supplier shall obtain from the applicable third party for the Customer's benefit, an irrevocable, perpetual, non-exclusive, worldwide, royalty-free license, solely for Customer's internal business purposes; likewise, with respect to any Supplier Intellectual Property embodied or reflected in the Work Product or

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

- 12.9** Supplier agrees that it shall have written agreement(s) that are consistent with the provisions hereof related to Work Product and Intellectual Property Rights with any employees, agents, consultants, contractors or subcontractors providing services or Work Product pursuant to the Contract, prior to the provision of such services or Work Product and that it shall maintain such written agreements at all times during performance of this Contract which are sufficient to support all performance and grants of rights by Supplier. Copies of such agreements shall be provided to the Customer promptly upon request.
- 12.10** To the extent not inconsistent with Customer's rights in the Work Product or other provisions, nothing in this Contract shall preclude Supplier from developing for itself, or for others, materials which are competitive with those produced as a result of the services provided under the Contract, provided that no Work Product is utilized, and no Intellectual Property Rights of Customer therein are infringed by such competitive materials. To the extent that Supplier wishes to use the Work Product or acquire licensed rights in certain Intellectual Property Rights of Customer therein in order to offer competitive goods or services to third parties, Supplier and Customer agree to negotiate in good faith regarding an appropriate license and royalty agreement to allow for such.
- 12.11** If any Acquisition pursuant to the Contract is funded wholly or in part with federal funds, the source code and all associated software and related documentation and materials owned by a Customer may be shared with other publicly funded agencies at the discretion of such Customer without permission from or additional compensation to the Supplier.

13 Hosting Services

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

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

14 Change Management

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

15 Service Level Deficiency

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

16 Notices

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

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

With a copy, which shall not constitute notice, to:

Information Services Deputy Counsel
3115 North Lincoln Boulevard
Oklahoma City, Oklahoma 73105

Appendix 1 to State of Oklahoma Information Technology Terms

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

A. Customer Data

1. Customer will be responsible for the accuracy and completeness of all Customer Data provided to Supplier by Customer. Customer shall retain exclusive ownership of all Customer Data. Non-Public Data and Personal Data shall be deemed to be Customer's confidential information. Supplier shall restrict access to Customer Data to their employees with a need to know (and advise such employees of the confidentiality and non-disclosure obligations assumed herein).
2. Supplier shall promptly notify the Customer upon receipt of any requests from unauthorized third parties which in any way might reasonably require access to Customer Data or Customer's use of the Hosted environment. Supplier shall notify the Customer by the fastest means available and also in writing pursuant to Contract notice provisions and the notice provision herein. Except to the extent required by law, Supplier shall not respond to subpoenas, service or process, Freedom of Information Act or other open records requests, and other legal request related to Customer without first notifying the Customer and obtaining the Customer's prior approval, which shall not be unreasonably withheld, of Supplier's proposed responses. Supplier agrees to provide its completed responses to the Customer with adequate time for Customer review, revision and approval.
3. Supplier will use commercially reasonable efforts to prevent the loss of or damage to Customer Data in its possession and will maintain commercially reasonable back-up procedures and copies to facilitate the reconstruction of any Customer Data that may be lost or damaged by Supplier. Supplier will promptly notify Customer of any loss, damage to, or unauthorized access of Customer Data. Supplier will use commercially reasonable efforts to reconstruct any Customer Data that has been lost or damaged by Supplier as a result of its negligence or willful misconduct. If Customer Data is lost or damaged for reasons other than as a result of Supplier's negligence or willful misconduct, Supplier, at the Customer's expense, will, at the request of the State, use commercially reasonable efforts to reconstruct any Customer Data lost or damaged.

B. Data Security

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

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

2. All Personal Data and Non-public Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of Personal Data.
3. Supplier represents and warrants to the Customer that the Hosting equipment and environment will be routinely checked with a commercially available, industry standard software application with up-to-date virus definitions. Supplier will regularly update the virus definitions to ensure that the definitions are as up-to-date as is commercially reasonable. Supplier will promptly purge all viruses discovered during virus checks. If there is a reasonable basis to believe that a virus may have been transmitted to Customer by Supplier, Supplier will promptly notify Customer of such possibility in a writing that states the nature of the virus, the date on which transmission may have occurred, and the means Supplier has used to remediate the virus. Should the virus propagate to Customer's IT infrastructure, Supplier is responsible for costs incurred by Customer for Customer to remediate the virus.
4. Supplier shall provide its services to Customer and its users solely from data centers in the U.S. Storage of Customer Data at rest shall be located solely in data centers in the U.S. Supplier shall not allow its personnel or contractors to store Customer Data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. Supplier shall permit its personnel and contractors to access Customer Data remotely only as required to fulfill Supplier's obligations under the Contract.
5. Supplier shall allow the Customer to audit conformance to the Contract terms. The Customer may perform this audit or contract with a third party at its discretion and at Customer's expense.
6. Supplier shall perform an independent audit of its data centers at least annually at its expense and provide a redacted version of the audit report upon request. Supplier may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.
7. Any remedies provided in this Appendix are not exclusive and are in addition to other rights and remedies available under the terms of the Contract, at law or in equity.

C. Security Assessment

1. The State requires any entity or third-party Supplier Hosting Oklahoma Customer Data to submit to a State Certification and Accreditation Review process to assess initial security risk. Supplier submitted to the review and met the State's minimum security standards at time the Contract was executed. Failure to maintain the State's minimum security standards

during the term of the contract, including renewals, constitutes a material breach. Upon request, the Supplier shall provide updated data security information in connection with a potential renewal. If information provided in the security risk assessment changes, Supplier shall promptly notify the State and include in such notification the updated information; provided, however, Supplier shall make no change that results in lessened data protection or increased data security risk. Failure to provide the notice required by this section or maintain the level of security required in the Contract constitutes a material breach by Supplier and may result in a whole or partial termination of the Contract.

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

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

1. Supplier may need to communicate with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Contract. If a Security Incident involves Customer Data, Supplier will coordinate with Customer prior to any such communication.
2. Supplier shall report a Security Incident to the Customer identified contact set forth herein within five (5) days of discovery of the Security Incident or within a shorter notice period required by applicable law or regulation (i.e. HIPAA requires notice to be provided within 24 hours).
3. Supplier shall:
 - a. Maintain processes and procedures to identify, respond to and analyze Security Incidents;
 - b. Make summary information regarding such procedures available to Customer at Customer's request;
 - c. Mitigate, to the extent practicable, harmful effects of Security Incidents that are known to Supplier; and

d. Document all Security Incidents and their outcomes.

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

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

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

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

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

F. Notices

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

Chief Information Security Officer

3115 N. Lincoln Blvd

Oklahoma City, OK 73105

and

servicedesk@omes.ok.gov.

G. Supplier Representations and Warranties

Supplier represents and warrants the following:

1. The product and services provided in connection with Hosting services do not infringe a third party's patent or copyright or other intellectual property rights.
2. Supplier will protect Customer's Non-Public Data and Personal Data from unauthorized dissemination and use with the same degree of care that each such party uses to protect its own confidential information and, in any event, will use no less than a reasonable degree of care in protecting such confidential information.
3. The execution, delivery and performance of the Contract and any ancillary documents and the consummation of the transactions contemplated by the Contract or any ancillary documents by Supplier will not violate, conflict with, or result in a breach of any provision of, or constitute a default (or an event which, with notice or lapse of time or both, would constitute a default) under, or result in the termination of, any written contract or other instrument between Supplier and any third parties retained or utilized by Supplier to provide goods or services for the benefit of the Customer.
4. Supplier shall not knowingly upload, store, post, e-mail or otherwise transmit, distribute, publish or disseminate to or 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.

H. Indemnity

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

opinion, be likely to become the subject of a claim or an injunction preventing its use as contemplated in connection with Hosting services, Supplier may, at its option (i) procure for the State the right to continue using the software or (ii) replace or modify the software with a like or similar product so that it becomes non-infringing.

I. Termination, Expiration and Suspension of Service

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

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

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

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

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

c. a combination of the two immediately preceding options.

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

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

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

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

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

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

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

Appendix 2 to State of Oklahoma Information Technology Terms

INTRODUCTION

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

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

CJIS SECURITY POLICY REQUIREMENTS GENERALLY

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

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

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

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

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

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

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

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

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

Policy Requirement Checklist

Compliance checklist –

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

Attachment E-1 Price

Exhibit 4

Services - Tiered Pricing/Consumption Based Pricing

SW1118 Call Contact Center

Description	Unit of Measure	List Price	% off List Price	Cost per Unit
Call Center Manager	Hour	\$ 73.87	0 \$	73.87
Call Center Supervisor	Hour	\$ 56.05	0 \$	56.05
Customer Service Lead	Hour	\$ 41.64	0 \$	41.64
Customer Service Representative	Hour	\$ 39.58	0 \$	39.58
Quality Specialist	Hour	\$ 41.64	0 \$	41.64
Trainer	Hour	\$ 54.07	0 \$	54.07
Helpdesk	Hour	\$ 54.07	0 \$	54.07



ATTACHMENT E-2 RESPONSE TO SPECIFICATIONS

i. Ability to Meet or Exceed Any Acquisition Specifications

Our response to each of the items requested in Section 8.1.C of the RFP follows.

1. List and Briefly Describe the Areas of Specialty

We are distinctively qualified to administer a high-performing call center for OMES. We operate several call centers across the country for programs of various sizes. The services we support through these call centers reflect our areas of specialty and include information and referral services, comprehensive education, eligibility screening for various programs, status inquiry, benefit inquiry, enrollment into available programs, complaint resolution, and countless others.

State and local government organizations similar to OMES are the majority of our customers. Our current clients are described in Exhibit 1. These clients demonstrate that our tools and processes are scalable and flexible to meet growing demands. All current contracts include a significant call center component.

Exhibit 1. Current Contracts

Client	Type of Contract	Duration	Peak Staffing	Calls/Mo	Description
North Carolina Division of Economic Security	Unemployment Center	2021- Present	100	18,000 ¹	<ul style="list-style-type: none"> Unemployment insurance call center
HealthSource Rhode Island	Exchange Contact Center	2016- Present	230	50,000	<ul style="list-style-type: none"> Application, eligibility, and enrollment support into a healthcare program
Division of TennCare	Eligibility and Application Assistance	2014- Present	300	40,000	<ul style="list-style-type: none"> Information, education, and referral services on the State's available health and social programs Application assistance and processing Document intake
Florida Agency for Health Care Administration	Medicaid Enrollment Broker	2010- Present	500	50,000	<ul style="list-style-type: none"> Enrollment services Outbound mail fulfillment Referral to available resources and support
Ohio Department of Medicaid	Medicaid Hotline Enrollment Broker	1998- Present	200	250,000	<ul style="list-style-type: none"> Hotline that provides education, information, and referral services on relevant programs Enrollment services Outbound mail fulfillment
Delaware Health and Social Services	Medicaid Enrollment Broker	2019- Present	15	3,500	<ul style="list-style-type: none"> Enrollment services Outreach services Outbound mail fulfillment

¹ AHS will take 40,000 calls per month beginning in the summer of 2022.



Client	Type of Contract	Duration	Peak Staffing	Calls/Mo	Description
Nebraska Department of Health and Human Services	Medicaid Enrollment Broker	2016-Present	15	1,500	<ul style="list-style-type: none"> Enrollment services
Wyoming Department of Health	Medicaid Application Intake and Support	2020 – Present	50	10,000	<ul style="list-style-type: none"> Information, education, and referral services on the State’s available health and social programs Application assistance and processing Document intake
Massachusetts Call Center	Eligibility, Medicaid Enrollment Broker, Provider Services	2021-Present	150	16,000 ²	<ul style="list-style-type: none"> Information, education, and referral services on the State’s available health and social programs Application assistance Enrollment services
St. Louis Regional Health Commission	Eligibility and Application Assistance	2011-Present	15	1,500 ³	<ul style="list-style-type: none"> Application, eligibility, and enrollment support into a subsidized healthcare program
Maryland Department of Health	Medicaid Provider Enrollment	2017-Present	70	5,000	<ul style="list-style-type: none"> Information and education on provider enrollment protocols and requirements Enrollment assistance Outreach services Outbound mail fulfillment
Missouri Department of Social Services	Eligibility, Medicaid Enrollment Broker, Provider Services	2021-Present	150	N/A ⁴	<ul style="list-style-type: none"> Information, education, and referral services on the State’s available health and social programs Application assistance Enrollment services Outbound mail fulfillment

Our current contracts are similar to the services required by OMES.

Additional areas of specialty include:

- Mail fulfillment
- Document scanning and processing
- Field operations/outreach

2. Account Team Capabilities

During the initial contract process, we work our clients to define the scope of work, requirements, and anticipated call volumes. We use this information to develop a contract-specific staffing model. Based on the anticipated size of the workforce, we determine the

² The contract was implemented on a staggered basis. The volume of calls AHS is accepting increases each month.

³ The Project is in its close out phase.

⁴ The Project launched on July 11, 2022. Call data is not yet available.



appropriate management infrastructure needed to oversee the Project. For example, in our TennCare Connect contract, we employ approximately 300 staff, consisting of CSRs, Lead CSRs, Supervisors, and Managers. We also have the following key positions in place: Executive Director, Operations Directors (2), Operations Manager, Training Manager, Quality Assurance Manager, Workforce Manager, Document Center Manager, and Human Resources Director. In another example, in our Florida Enrollment Broker contract, we employ approximately 80 staff consisting of CSRs, Lead CSRs, Supervisors, and mail staff. We also have the following key positions in place: Account Manager, Call Center Manager, IT Manager, and Mailroom Manager.

Any project resulting from a contract for this RFP will be overseen by an Operational Vice President who will have executive-level responsibility for the Project. This Operational Vice President will serve as the primary Point of Contact (POC) between AHS and the State of Oklahoma, as well as oversee and perform account management activities.

Mr. John Fields, PMP, MPS, is one of our operational Vice Presidents. He represents the caliber of skill and experience of the individual who will oversee a contract. Mr. Fields is an executive-level project manager with more than 20 years of experience managing and supporting the successful execution of large-scale projects in the government and private sectors. Mr. Fields has more than 10 years of leadership experience in Call Center operations and seven years of experience working with Tennessee, which includes the successful implementation and administration of large-scale Call Center and document management processes.

We will assign a Call Center Manager to oversee the day-to-day activities of the contract. This individual will have the authority to make decisions and resolve problems. The Call Center Manager will have direct access to our Senior Executive Team and will be able to quickly engage AHS leadership for additional support and rapid problem resolution, if needed.

We will assign a Technical Team to support the CRM configuration and any integrations with OMES systems. The Technical Team will configure, install, and implement any technologies needed for the contract. Our Vice President of IT will oversee any IT efforts in coordination with this team and OMES.

Our Vice President of Telecommunications will liaise with OMES regarding any needed support for NICE CXone.

Based on the size, complexity, scope of work, and related requirements for the contract, common positions typically assigned to a contract include but are not limited to:

- Trainers
- Call Center Supervisors
- Lead Customer Service Representatives (Lead CSRs)
- Customer Service Representatives (CSRs)
- Quality Analysts
- Administrative Assistants
- IT Analysts
- HR Personnel



The contract is overseen and guided by our Senior Executive Team. Brief bios of our Senior Executive Team members are provided in Exhibit 2.

Exhibit 2. Senior Executive Team Qualifications and Involvement

Member	Biography
<p>Moses Haregewoyn, EdD, MBA, MPH President</p>	<p>A seasoned professional, accomplished leader, and well-respected administrator with proven business and policy development skills and experience, Dr. Haregewoyn has directed and overseen our statewide Ohio program since 1999, and now serves as AHS President. He holds an EdD in Organizational Behavior, an MBA, and an MPH. In any endeavor he undertakes, he bears ultimate responsibility for its execution and completion. Dr. Haregewoyn will assume ultimate responsibility for all facets of the implementation and ongoing contract service delivery for the Call Center Project. He will work closely with all parties to ensure the contract is executed on-time and will direct the Senior Executive and Project Teams to ensure work progresses according to contract standards.</p>
<p>Joseph P. Cain III, CPA Chief Financial Officer, Secretary, Treasurer</p>	<p>Mr. Cain has more than 25 years of experience in managing day-to-day financial operations and has demonstrated excellent financial management and accounting skills. With AHS since 2014, he provides all financial management, budgeting, and accounting functions necessary for AHS corporately and across all projects. Mr. Cain’s background includes extensive hands-on experience providing fiscal responsibility for accurate and timely delivery of all tax, consulting, and financial-related projects and preparation of annual corporate budgeting. Having worked in various leadership roles, his experience provides him with a broad-based background in business operations with increasing levels of responsibility. For the Call Center Project, Mr. Cain will provide oversight for all financial-related functions.</p>
<p>Kimberly A. Conner, MS Executive Senior Vice President of Human Resources, Training and Development</p>	<p>Before joining AHS in 1994, Ms. Conner was involved in hospital/health care delivery systems for 17 years, with an overall emphasis on management and staff training. She handles personnel issues, staff recruitment, initial training, and ongoing development (particularly in the areas of confidentiality, employee performance evaluations, policies, and procedures). For the Call Center Project, Ms. Conner will be responsible for recruiting, screening, and hiring activities of Project staff in consultation with Project management. She will ensure that all staff are fully hired, trained, and capable of providing outstanding, culturally competent services to callers.</p>
<p>William V. Williams Senior Vice President of Strategic Business Development and Sales</p>	<p>Mr. Williams possesses more than 30 years of experience working closely with State human services agencies to develop management and IT solutions that enable the most effective administration and expansion of these programs. A graduate of West Point Military Academy, Mr. Williams draws on a wide ranging, in-depth background to develop and provide valued management and solutions for State governments, payers, and public entities.</p>
<p>Robert Doran Vice President of Telecommunications</p>	<p>Mr. Doran has been with AHS since 1986. He has 30 years’ experience with human services administration and over 20 years’ experience administering telecommunication systems for our multi-state contact center operations. Mr. Doran ensures the appropriate selection, installment, and functioning of each of our Projects’ telecommunication solutions. Mr. Doran will provide necessary telephone support.</p>
<p>Eng Tan, MS, CPHIMS Vice President of Information Technology</p>	<p>Mr. Tan has more than 15 years’ experience working with various State systems as well as interfacing with a range of third-party computer systems. He currently oversees all operations related to application design, development, testing, and implementation, as well as all network, data transfer and interface connectivity activities necessary for all our projects. He is also responsible for all computer hardware and software procurement and aligns IT solutions with business needs. For the Call Center Project, Mr. Tan will direct the configuration of our CRM and establish any integrations with OMES systems.</p>



Member	Biography
<p>Derek Jackson, MSOL Vice President</p>	<p>Mr. Jackson is a seasoned manager with more than 25 years of proven leadership experience. He has an extensive background in Florida Medicaid services, including responsibilities for the overall management and operation of Fiscal Agent Contracts. He holds a Master’s in Science in Organizational Leadership and is a Certified Six Sigma Greenbelt well versed to lead large-scale operations to ensure maximum efficiencies. Currently, he works closely with our Florida client and achieves performance and quality standards. Mr. Jackson will provide support and guidance as needed.</p>
<p>Christine DiFrancesco, PMP Vice President</p>	<p>Ms. DiFrancesco is a highly accomplished leader with more than 15 years of relevant experience in health and human services program administration and 10 years of hands-on management experience for several call center, mail fulfillment, and document processing contracts, including statewide contracts in Illinois, Tennessee, Rhode Island, Wyoming, Missouri, and North Dakota. She has led additional large-scale contracts for Cook County, Illinois, and directed over ten statewide contract implementations. Ms. DiFrancesco will provide assistance, consultation, and support as needed.</p>
<p>John Fields, PMP Vice President</p>	<p>Mr. Fields, PMP, is an executive-level project manager with more than 20 years of experience managing and supporting the successful execution of large-scale projects in the government, health care, and private sectors. Mr. Fields has over 10 years leadership experience in Contact Center operations and five years of experience working with Tennessee Medicaid, which includes the successful implementation and administration of large-scale onsite and virtual contact center and document management processes. Mr. Fields has more than seven years’ experience administering high performing contracts in the State of Tennessee – all with excellent results and high performance. He will provide assistance, consultation, and support, as needed.</p>
<p>Rebecca Matthews Vice President of Marketing and External Affairs</p>	<p>Ms. Matthews leads strategy development and execution to promote the success of a comprehensive program of services offered by AHS. Ms. Matthews represents AHS before policy makers, government and regulatory bodies, trade organizations, corporate entities, and other key stakeholders at the national, State, and local levels. Prior to joining AHS, Ms. Matthews served as Chief Executive Officer of the Florida Healthy Kids Corporation. She led product development, health and dental plan contracting, and oversight of operations of Florida Healthy Kids, a program that provides low-cost health insurance for children ages 5-18 who do not qualify for subsidized coverage. For the Call Center Project, she will provide support as needed, including representing AHS to the State’s policy makers and supporting strategic planning as appropriate.</p>

Our Senior Executive Team is prepared to support the Project throughout its duration.

3. Documented Escalation Process

We have two common escalation processes. First, we have a documented approach to security incidents. Second, we have a documented process for call escalations.

Incident Escalation Process

We have a detailed security incident reporting process that prompts timely and transparent communication with OMES. The Call Center Manager will have ultimate accountability for all issues requiring escalation.

The steps involved are as follows:

- The IT Department and Call Center Manager are notified of an incident or problem. The Call Center Manager performs an initial assessment of the issue and notifies the Escalation Response Team.



- The Escalation Response Team examines the information about the situation and determines if an incident or problem has occurred. If an incident has occurred, they determine the nature of the incident, assess the severity, and assign an initial priority level, based on the category and nature of the problem.
- The Escalation Response Team determines an appropriate course of action.
- The Call Center Manager notifies OMES of the crisis, including the time of the incident, the severity, the action steps put in place, and the expected resolution timeframes. Notification will occur via phone and email. The Call Center Manager will remain available to OMES for ongoing updates.
- The Escalation Response Team will limit the scope and magnitude of the incident to keep the incident from getting worse. If appropriate, the Escalation Response Team will consider system backup, the risk of continuing services, changing access controls, etc.
- The Escalation Response Team will determine the cause of the incident.
- The Escalation Response Team will restore the business and operational processes. Actions may include restoring and validating system and monitoring operations to verify normal operations are in place. The Escalation Response Team addresses any security gaps.
- The Escalation Response Team prepares and submits incident reports to OMES, which include lessons learned from the incident handling process, successful and unsuccessful actions taken in response to the incident, and recommendations to prevent future incidents and improve the overall enterprise operations. The Call Center Manager will work with OMES to provide any details that may need to be provided.
- The Call Center Manager will update the Incident and Escalation Procedure following each incident and on an annual basis. The Call Center Manager will submit all changes to the OMES for approval. The Call Center Manager closely monitors the updated processes to ensure they are addressing the issue.

Call Center Escalation Process

Calls needing to be escalated for advanced resolution are assigned an initial priority level based on the category and nature of the problem. The escalation procedures involve the following levels:

Level 1

- The CSR calls the Supervisor and transfers the call to the Supervisor for resolution.
- When instructed to by the Lead/Supervisor, the CSR sends the issue through the CRM and informs the caller that the Supervisor will return the call as soon as possible.
- The call is then escalated to Level 2.

Level 2

- The Supervisor returns the call to the customer and works to de-escalate the issue.
- The Supervisor logs all work done with/for the customer in the CRM.
- If the Supervisor determines the Call Center Manager's intervention is needed, the call escalates to Level 3.



Level 3

- The Supervisor discusses the case information with the Call Center Manager and all actions performed to resolve the issues on the case. The Call Center Manager and the Supervisor discuss other possible steps to try to resolve the caller’s issues.
- The Call Center Manager speaks directly with the caller to attempt to resolve the issues.
- The Call Center Manager documents all interactions with the customer in the CRM.
- If resolution of the problem is still not achieved and the Call Center Manager requires intervention from other departments, the call is escalated to Level 4.

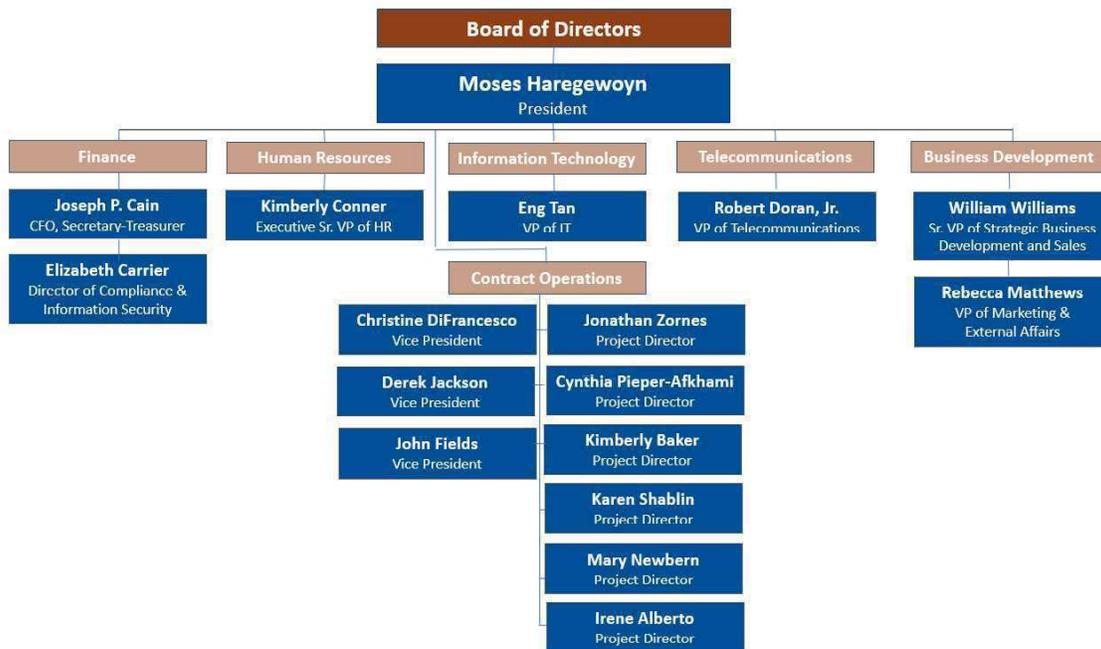
Level 4

- The Call Center Manager determines assistance is needed from the Operational Vice President. The Call Center Manager works directly with the above parties to find resolution. If necessary, the Call Center Manager discusses the case with OMES staff as part of the resolution process.
- The Call Center Manager speaks with the customer to discuss the resolution OMES can provide. The Call Center Manager documents all interactions with the caller in the CRM.

4. Copy of Current Company Organizational Chart

Our current organizational chart is provided in Exhibit 3.

Exhibit 3. Company Organizational Chart



Our organization is logically structured with clear lines of authority.

5. Time Keeping Procedures and Verification Practices

Non-exempt employees are required to track their time in ADP when beginning their work day, leaving and returning from lunch, and leaving at the end of the work day, which is the basis for their pay. Supervisors are tasked with comparing logged time in ADP and NICE CXone to ensure staff are appropriately productive.



6. Number of Employees and Areas of Specialty

AHS employs approximately 1,300 individuals nationwide. All our employees provide a variety of professional, operations, information technology, systems, telecommunications, and front-line engagement for a multitude of projects—all similar in scope.

These individuals include experts in:

- **Human Resources (HR):** Our HR Team, consisting of HR Generalists, Recruiters, etc. supports the ongoing hiring and management of employees.
- **Information Technology (IT):** Our IT Team, consisting of Developers, Business Analysts, Systems Testers, etc. is responsible for configuring our CRM to meet the specifications of our clients. The IT Team also ensures that proper software is available, security standards are maintained, and ongoing user support is provided.
- **Telecommunications:** Our Telecommunications Team, consisting of Telecommunications Analysts and support personnel, is responsible for leading the configuration, deployment, and ongoing maintenance of our telecommunications solution. In contracts where our clients provide the telecommunications system, our Telecommunications Team liaises with our client’s team to provide ongoing information concerning the health of the system.
- **Project Teams:** As mentioned, each Project Team is specifically constructed based on the scope of work for the respective contract. Project Teams develop specific subject matter expertise based on the scope of the contract and typically include a team of Managers, Supervisors, Lead CSRs, CSRs, and appropriate support personnel (e.g., Quality Analysts, Administrative Assistants, etc.).

7. How Work is Completed Remotely

During the COVID-19 pandemic, all of our call centers operated remotely for various periods. Additionally, several of our call centers use a dual location model for disaster recovery and redundancy purposes. Currently, all of our call centers have a variable contingent of their workforce operating in a remote capacity. This experience provides us with proven policies and procedures, lessons learned, and best practices related to remote operations. Our approach includes the components identified in Exhibit 4.

Exhibit 4. Remote Work

Component	Description
Technical Tools	<ul style="list-style-type: none"> • We use several technical tools to foster effective remote work: <ul style="list-style-type: none"> – Microsoft Teams for collaboration and communication – SharePoint for document and policy sharing – OneDrive for cloud storage • All operational systems (e.g., CRM, knowledgebase, etc.) are cloud-based
Security	<ul style="list-style-type: none"> • We have multiple tools in place to protect our systems <ul style="list-style-type: none"> – Cato SD-WAN – Arctic Wolf for digital denial of service and other security monitoring components – VPN and MFA for secure access to multiple systems • All staff participate in initial and annual privacy and security training
Policies	<ul style="list-style-type: none"> • We have multiple policies that guide work from home practices: <ul style="list-style-type: none"> – Technical Resources – Work from Home Policies – Security Policies



Component	Description
	<ul style="list-style-type: none"> – Company Property – Mobile Device Security
Quality Monitoring	<ul style="list-style-type: none"> • Staff are required to adhere to AHS requirements for ongoing quality monitoring – Staff are provided with needed refresher training and links to corrective feedback – Staff may be required to return to their nearest AHS office for close supervision if needed
Communication	<ul style="list-style-type: none"> • Staff participate in multiple team meetings <ul style="list-style-type: none"> – We institute team huddles at the start of the day to foster a spirit of collaboration – Supervisors conduct regular team meetings via Microsoft Teams – Staff are required to participate in regular check-ins with their Supervisor or Manager and to video display if needed • We have multiple forms of ongoing communication: <ul style="list-style-type: none"> – Ongoing staff emails – Knowledgebase alerts and updates – CRM announcements
Tracking	<ul style="list-style-type: none"> • Supervisors and Managers have remote access to all programs and quality metrics • Supervisors and Managers track all performance statistics on an ongoing basis • Time and attendance is tracked through ADP

We have several factors that contribute to a successful remote work environment.

8. Responsible for Background Checks and Training. Explain Staffing Resource Management Plan

Background Checks

We routinely perform background checks on new hire candidates. We do not hire candidates with unacceptable background checks. Background check results can be provided to OMES upon request. Additional details on which background checks we perform are provided in the following question.

Training

Our approach to training is provided in detail in Section Eight, question 12.

Staffing Resource Management Plan

Staffing resource management is a major factor in the success of our contracts. We have a multi-step process to correctly determine the numbers and types of employees required to complete tasks and fulfill contractual obligations throughout significantly fluctuating volumes of our contracts. By basing staffing plans on thorough data analysis, projections, and years of hands-on project administration experience, we are confident our proposed staffing plans are fully responsive to the needs of the projects we administer. We assess the various programmatic requirements and scope of services required for each phase of the Project. We take pride in successfully forecasting the size of the workforce, hiring qualified, culturally competent, and sensitive staff with relevant experience in customer service, and retaining excellent personnel.



We will conduct thorough analyses to ensure we have the correct mix of employees to complete the tasks identified in the contract. To guarantee we establish the right number and types of staff, as well as the best skillsets to serve OMES and the Project’s callers, we will consider all available data (including volumes, scope of work, performance standards, etc.), apply our full corporate experience, and use a proven software solution when determining our staffing plans.

We will hire both full- and part-time staff for customer-facing positions to increase our flexibility and ability to respond appropriately for anticipated and unanticipated changes in Call Center Project activity. Our approach to workforce management supports efficient Project staffing and allows us to determine accurate staff schedules to meet SLAs. We will use multiple methods to determine staffing that consider historical data, operations, communication channels, workflows, efficiencies, timelines, and individual needs of the Project, while leveraging our corporate experience and workforce management system.

As a result, our staffing projects are maximally accurate because our approach:

- Allows for expertise in critical subject matter areas
- Considers service level and performance requirements of the RFP
- Considers intraday variability (e.g., projected peak and off-peak times)
- Supports the use of more sophisticated and efficient staffing patterns (e.g., utilizing a complement of quality staff to meet peaks)

Our staffing model provides full oversight by a team of Supervisors and Lead CSRs, as well as a complement of quality staff to monitor and ensure high performance.

9. Which Screening Activities are Performed

- Criminal history background check **YES**
- Employment verification **YES**
- Reference checks **YES**
- Review of skills **YES**
- Review of job duties at most recent placement(s) **YES**
- Reason for leaving last assignment **YES**
- Availability **YES**

10. Time to Fill a Vacant Position

We commend OMES for recognizing the challenges associated with fluctuating volumes. As call volumes dynamically change, we have several strategies we can implement to ensure continued service. For example, we use a complement of part-time staff that can immediately expand their hours to increase our FTE capacity when needed.

Did You Know?

We are proud of our ability to provide expert staff with high capabilities who support our clients with significant initiatives. Our TennCare Connect Project is representative of the caliber of talent we provide to jointly achieve our clients’ vision. In this Project, our staff achieved several impressive accomplishments, including but not limited to:

- Supported TennCare with critical initiatives that resulted in accurate service during a litigious time at the start of our contract
- Supported TennCare’s monumental efforts to launch TEDS
- Achieved high performance and SLA attainment



In the event of an employee separation, we activate our pipeline to quickly fill a vacant position. The time to fill a vacant position varies depending on the position and number of vacancies. For example, filling a small number of CSR positions (e.g., less than 10) can be done in less than one week on average; filling a larger number of CSR positions or supervisory/management positions will take on average at least two weeks.

11. Risks Associated with Filling a Position and Mitigation Plans

With any project, there is the risk of not having enough qualified CSRs, supervisors, and/or project managers necessary to properly staff and manage the project, which can lead to failure to meet the terms of any SLA.

Our approach to mitigating this risk focuses on:

- **Selection:** Our efforts begin with careful employee selection, which ensures we recruit staff with appropriate skills, education, and relevant backgrounds, as well as the enthusiasm and commitment to serve the Project. We look for personality characteristics in candidates that result in the best fit employees.
- **Analytics:** We analyze data on employees' attendance and performance. For example, employees with dips in their attendance, quality, or productivity scores may be dissatisfied and preparing to find a new position. We are acutely tuned into these signs so that we can either counsel the employee and identify causes of dissatisfaction and/or request that Human Resources intervene or examine our pipeline to ensure we have a pool of resources who can be contacted if needed so that no SLAs are in jeopardy.
- **Pipeline:** We constantly recruit and maintain a full pipeline of candidates on an ongoing basis to keep the Project fully staffed. The pipeline consists of both internal staff who have demonstrated they are ready to be promoted and prospective external candidates.
- **Recruiting Network:** We establish and maintain a solid network of partners who are prepared to refer potential candidates to us.
- **Retention:** Our approach to retention is based on proven practices that we utilize across our organization. We combine these practices with an ongoing analysis of retention rates and the effectiveness of our strategies. We continuously adapt our strategies in response to the specific demographics and culture of the State of Oklahoma and emerging needs of any project. We provide a team of trained and engaged staff who are excited to serve the Project to maximize staff retention. Retaining talented staff results in better customer service delivery and an enhanced ability to respond to changing project needs, as well as reduced turnover costs.
- **Training:** We have comprehensive training plans to provide clear expectations for job performance, skills, and knowledge needed, which is instrumental in our retention efforts. We provide ongoing trainings that keep skill levels high and ensure that staff members are challenged and engaged in job performance. This training program consists of a structured 90-day orientation period and provides guidance to new employees as they navigate the environment of AHS and the nuances of a specific project. It provides clear expectations and guidelines on what is required to be successful in their positions. Our training plans have defined touch points at 30, 60, and 90 days to gauge their satisfaction and provide



feedback on their performance. We couple this training with a nesting period where staff have access to support and frequent monitoring to reinforce excellent work habits.

- **Staff Redeployment:** When available and appropriate, CSRs assigned to other projects can be redeployed to assist State of Oklahoma projects. In addition, management and supervisory roles can be filled at the corporate level.

12. Company Procedures

We have strong practices for all areas of call center operations.

a. Staff Management

We design staffing models based on the anticipated volumes, work levels, and scope of services for each contract. Staffing models include a full complement of necessary supervisory, training, and quality assurance staff. We have multiple feedback loops among these various teams to provides full communication and coordination regarding staff needs. For example, if Supervisors or quality staff identify ongoing issues related to a specific topic, they share this information with the Training Team so that initial training can be bolstered, ongoing training modules can be distributed, and the knowledgebase can be updated.

We model our staffing plan with industry standard ratios of Supervisors to CSRs. These ratios are strengthened by the role of Lead CSRs who assist the Supervisors and perform on-the-floor mentoring, support, coaching, etc. They also address complex calls. Supervisors are tasked with ongoing feedback and communication to CSRs and have defined meetings at 90 and 180 days, which provides needed opportunities to review performance and quality results and discuss plans for growth and career building. (These meetings complement the routine training meetings at 30, 60, 90, and 180 days.)

A key component of our staff management approach is our Quality Improvement (QI) Plan, which we use to ensure staff are optimally performing their tasks, managing workload effectively, growing in their positions, and representing the Project to the expectations for AHS and OMES. Quality monitoring activities will also serve as an early warning system so that any problem can be detected and promptly (and permanently) corrected.

Did You Know?

While a key goal of our QI Plan is to identify and immediately address undesirable deviations from quality standards, we recognize that it is vital for staff morale and performance to reward staff for good performance. We incorporate tools that recognize excellent performance to keep staff motivated and engaged.

There are multiple components that we will integrate into the QI Plan related to staff management for this Project:

- Policies and Procedures
- Training
- Operational Monitoring
- Performance Metrics Monitoring
- Corrective Disciplinary Action Follow-Up
- Incentives



Policies and Procedures

Policies and procedures will underlie all operational workflows for the call center. Policies and procedures will be incorporated into our QI Plan and integrated into the knowledgebase following approval. Policies and procedures address staff management, including disciplinary steps when needed.

Training

Training is a fundamental component of our approach to ensuring quality services and is described later in this section.

Operational Monitoring

Monitoring staff performance is the backbone of our quality approach. We utilize a range of tools to monitor both systems and non-systems performance. We will discretely listen to calls and observe fluency in the CRM for CSRs. Staff will not be able to tell if they are being monitored. To objectively monitor staff performance, we will develop Evaluation Forms for performance assessment as shown in Exhibit 5. Each category is appropriately weighted.

Did You Know?

We currently use the quality tools available through NICE CXone to monitor staff in our TennCare Connect contract.

Exhibit 5. Evaluation Form for Call Center Operations

Topic	Items Assessed
Greeting and Verification	<ul style="list-style-type: none"> • Greeted the caller and verified who is calling • Verified relationship and asked appropriate relationship questions • Verified primary caller’s information
Call Purpose	<ul style="list-style-type: none"> • Identified/logged the purpose of the call • Followed appropriate script
Call Transfer	<ul style="list-style-type: none"> • Documented the name of agency/phone number if transferred • Documented all call transfers
Program Information	<ul style="list-style-type: none"> • Demonstrated accurate knowledge of policy
Call Actions	<ul style="list-style-type: none"> • Completed all call actions and entered correct notes in the CRM
Customer Service	<ul style="list-style-type: none"> • Demonstrated professional and courteous behavior and listened effectively • Asked appropriate probing questions • Thanked the caller
Systems Use	<ul style="list-style-type: none"> • Accessed the correct OMES system if appropriate for the type of caller • Managed the correct workflow and documentation
Documentation	<ul style="list-style-type: none"> • Completed the closing survey for caller type • Documented all actions in the CRM

Evaluation Forms are comprehensive.

Once the form is approved by OMES, we will implement the appropriate notifications to the CSR and Supervisor based on the results of the evaluation. Our solution includes:

- Immediate notifications to employees through customized emails with targeted trainings based on evaluation scores to trigger immediate results
- Notifications to the Supervisor of critical fails/urgent issues
- Flexible scoring to accommodate various scales (e.g., yes/no, 1-10, etc.)
- Weighting options
- Extensive analytics to carry out root-cause analysis and compare performance



Our goal is to immediately address and eliminate any issues that we identify during monitoring sessions. We configure the system flows based on OMES business rules. Flows are customized based on the specific deficiencies that were identified during the call. The quality staff completes the call monitoring, then uses the custom flows to email CSRs specific deficiencies that were identified, along with links to relevant training.

We developed our emails to include several components to further drive performance:

- Positive comments on items that scored well
- Courteous language (e.g., “please be mindful,” etc.)
- Direct links to assigned computer-based and video training
- Deadlines for completing training

We consider any missed item related to caller verification a critical fail/urgent issue. Whenever CSRs miss these items, an email is immediately sent to their Supervisors to alert them of the critical fail/urgent issue. We track and trend all missing topics and refine our training, knowledgebase, scripting, or system as appropriate to remediate any further issues.

Performance Metrics Monitoring

The Management Team will track and trend a range of statistics from NICE CXone and CRM to assess required metrics to ensure staff are operating effectively and supervisors are effectively managing their teams for high performance. Where possible and appropriate, we will have real-time notifications and alerts prior to missing a required performance metric so our Management Team can take immediate action regarding staff management (e.g., suspend time away for trainings, request part-time staff assist, etc.).

Corrective Disciplinary Action Follow-Up

We will implement appropriate corrective disciplinary actions, as needed. When a CSR receives a corrective disciplinary action (CDA), the Supervisor may require an increase in monitoring and/or side-by-side training for a set period as part of the corrective action plan to track improvement. The Management Team will be responsible for the appropriate monitoring and will complete the phone monitoring as requested, utilizing the Evaluation Form according to our monitoring procedures

Incentives

Where appropriate, we develop incentive programs to encourage desirable staff behaviors. Incentives are typically based on quality scores and attendance.

b. Staff Training

We are proud to prepare our staff to deliver outstanding service and equip them to enhance their skills and knowledge in an ongoing manner. As OMES’ programs transform over time, we adapt to the changing policy and program requirements, to achieve high levels of efficiency and to use technology to improve caller experience and first call resolution rates.

Representing OMES and the programs it serves in a professional, unbiased, culturally sensitive manner supports high levels of caller satisfaction and results in a positive experience with OMES’ programs. Staff must be prepared to serve OMES’ diverse callers and execute all tasks with accuracy. CSRs must understand the cultures, values, attitudes, and experiences across the State. Our training program meets these goals.



Out training program is comprised of three major types of training:

- **Initial Training:** The initial training program includes a New Hire training and orientation period that consists of active strategies and didactic sessions and concludes with an evaluation to assess readiness to perform operations.
- **Ongoing Development:** Ongoing trainings include targeted quality trainings that are conducted upon identification of an area for improvement. Ongoing trainings are also conducted on a routine basis for all staff to keep skills polished and provide staff with the most current information regarding Project and policy changes.
- **Continuing Education:** We offer a Professional Development series and provide tuition assistance to keep motivation levels high and support staff in advancing their careers.

Our training program includes an overview of the functions and mission of the OMES Call Center Project. We provide hands-on, practical, skill-based training for the Project. Training is paced to ensure retention of information and to develop service and system skills. We use a hybrid of computer-based training (CBT) modules and lectures as the base method of training, which we supplement with discussions and hands-on learning opportunities. Each module includes an assessment, and many include opportunities for role play. Where appropriate, we invite guest speakers to support us.

We integrate on-the-job scenarios throughout the training, which increase in difficulty as training progresses. These scenarios are incorporated into our final training assessment. We welcome OMES staff to attend, participate in, or deliver any training session. OMES participation is particularly helpful during the implementation so that OMES can verify that our training is aligned with OMES' vision. During the implementation period, we will work with OMES to develop the Training Plan and appropriate modules for the Call Center Project. Modules are designed to address all topics and are developed around SMART principles:

- **Specific:** The criteria clearly identify what percent of participants meet the objective and how they must meet it.
- **Measurable:** All criteria are measurable.
- **Achievable:** Training participants can reasonably achieve the objective.
- **Realistic:** Based on anticipated backgrounds and knowledge, it is realistic to expect participants to complete the objective following training.
- **Time-Specific:** We specify the timeframe to achieve the objective (e.g., after a completion of a module, the entire training session, hands-on practice, etc.).

Sample modules for the Call Center Project are detailed in Exhibit 6.

Exhibit 6. Training Curriculum

Module	Description
Call Center Project	Several modules summarize the Call Center Project for the State of Oklahoma.
Stakeholders	We address the stakeholders involved with the Call Center Project.
OMES Systems	We provide training on using any required State system. Training will address when to use each system and proper workflows and documentation within each system.
Security and Privacy 101	We stress the importance of protecting all information with which staff are entrusted. Relevant State and Federal laws, regulations, policies, and repercussions for breaches are discussed. Staff sign a confidentiality statement.



Module	Description
Quality and the Consumer	We review the definition of quality, elements of good service, and the cycle of improvement. We discuss the monitoring process and evaluation criteria.
Collaborative Work Skills	This module discusses the essentials of building relationships and constructively approaching and resolving conflicts (including crisis de-escalation).
Sensitivity Training	This module explains how to understand the complex health, physical, mental, and emotional factors that may affect callers. It helps staff understand various special needs populations, including persons with physical, sensory and/or cognitive disabilities, as well as persons with cultural and linguistic differences.
Embracing Diversity	This module provides strategies to consider when relating to people with other values, languages, cultures, disabilities, and/or experiences.
Complaints and Escalations	We address frustrated callers and appropriate customer service tips. The process to assist with filing a complaint is also covered and how and when to file an escalation.
Relevant IT Systems	Several sessions address hands-on understanding of our CRM and Microsoft Office programs. (OMES systems are addressed in a separate module.)
Phone and Communication Systems	Staff explore the full features of the phone system, including call transfers, referrals, hold features, use of Relay Services for hearing impaired callers, and accessing interpretation services.
Emergency Protocols	All types of emergencies are addressed, including how to respond to threatening or abusive phone calls, how to respond to threats of suicide, and our emergency evacuation procedures.
Ongoing Training	Refresher and quality training to ensure skill levels are high.

Our rigorous training program includes all needed topics.

We use video training to provide information to staff, reinforce key concepts, and build skills and proficiency. We have standardized our trainings on a CBT platform, ProProfs, as a complement to classroom-based learning. The ability of ProProfs to quickly create specific training to staff is essential as new changes are rolled out. We will be able to quickly develop new training material and circulate it to our staff without the challenges of removing our staff from the phones and experiencing detrimental effects to the Call Center SLAs.

ProProfs offers extensive advantages, including:

- **Supplement to initial trainings:** We can ask training participants to re-watch modules at any time on pertinent topics to reinforce essential skills and knowledge.
- **Easy integration with quality scores:** We can create modules on targeted topics to address any quality deficiencies—as soon as performance weaknesses are identified.
- **Enhanced learning and engagement:** CBT enhances engagement and retention.
- **Capitalization on learning for modern-day learners:** CBT responds to how new generations are accustomed to using YouTube and other internet resources to acquire skills. CBT allows to push out short bursts of material, which helps with knowledge retention.
- **Accommodate diverse shifts:** Part-time employees who may work non-traditional hours can still participate in training at times that align with their work cycles.



CSRs must complete the final post-test assessment prior to taking calls. The post-test assessment will include three parts:

- **Written and oral exam:** The written and oral exam will be highly comprehensive and will cover all learning objectives and topics presented in each module. We will use a variety of assessment strategies in the post-test assessment.
- **Successful demonstration of systems proficiency:** The practical test requires participants to demonstrate their proficiency with our CRM.
- **Successful demonstration of customer service:** Training participants must perform well in mock role play scenarios where they demonstrate customer service skills.

Did You Know?

We trained nearly 220 staff over the course of 2.5 weeks for the roll out of Florida's SMMC program. These staff achieved a pass rate of greater than 95%.

Participants must score 85% or higher on the post-assessment to pass. Participants who score below 85% will be given an additional opportunity to take the post-test assessment. After the initial training and nesting period ends, staff will continue to be engaged in learning activities through various delivery methods (e.g., check point/refresher training, team meetings, individual coaching, Lunch and Learns, mentorship program, program updates, continuing education, etc.).

We understand that in a dynamic government environment, there are instances when a last-minute change or emergency update must be made. In these instances, we can update all our materials and provide training within 24 hours. If such a situation arises, we will immediately draft the material, submit to OMES for approval, and upon receipt of approval, implement training. Training on such updates can be performed via alerts in our knowledgebase or CRM, email notifications, and small group sessions held throughout the day.

c. Ongoing Training and Support

We provide staff with continuing support and education as the staff completes the training period and begins operations. Following the evaluation test, we complete a nesting period and close supervision during a CSR's first days taking calls. During the nesting period, new training graduates have close access to more senior staff, Supervisors, and training support.

Following initial training, we implement ongoing training. Ongoing training consists of two components: quality improvement training and refresher training. All staff who do not meet the requirements outlined as part of our monitoring policy are required to attend quality improvement training as part of their CDA. Quality training is designed to provide intense, focused training in areas where the CSR scored poorly on their monitoring evaluation form. Quality training reinforces requirements of phone and task monitoring. Our capability to monitor staff in real time allows us the avenue to notify staff immediately if there is a critical need for additional training.

We will provide the CSR with immediate results of all notifications, as well as direct links to training. The CSR will be assigned to complete the appropriate training and pass an evaluation within a designated timeframe. The Supervisor and QA staff will monitor completion and evaluation results. If additional training is needed, additional measures may be implemented.



Refresher trainings are designed to reinforce important customer service and quality metrics. These creatively themed, interactive training sessions will reaffirm the quality approach all staff should take in their day-to-day activities and the principles they should carry through each interaction. Our ability to immediately update staff on key program changes and updates is essential to continuing to provide callers with accurate information. We will provide annual training on privacy, security awareness, and annual disaster recovery protocols, and any other key topics identified by OMES. In the event of promotions, additional training is provided to staff based on their new roles and responsibilities.

Refresher training may also include targeted programs to bolster professional skills. As an example, as part of ongoing training in one contract, we provide webinar training sessions through LinkedIn Learning, which offers presentations on various business, communication, and job skills by experts in that field (e.g., a business professor at Duke discussing leadership, etc.).

d. Assign Skill Level

Staff are assigned skills based on their languages and work responsibilities. For example, bilingual staff are assigned skills based on the languages spoken. Supervisors are assigned higher tier skills than CSRs so they can properly oversee CSRs, receive escalated calls, etc. When needed, we have specialized groups of staff assigned to specific topics.

e. Management of Day-to-Day Activities

The management of day-to-day activities is performed by our Management Team. Based on the size of the resulting contract, the team will consist of the Call Center Manager, Supervisors, Lead CSRs, and CSRs. Day-to-day activities are distributed throughout the Team accordingly based upon each role's function.

Call Center Manager

The Call Center Manager has responsibility for oversight and monitoring of the Call Center staff. This position participates in the development and implementation of training designed to maintain CSR knowledge of OMES programs, as well as to oversee their cultural competencies. This position monitors the overall performance of the Call Center in comparison to established performance metrics. This position oversees the day-to-day work of the Supervisors to ensure staff are appropriately scheduled to meet all contractual hours of operation. This position generates and reviews reports and monitors the ongoing operational performance of the team.

Supervisors

Supervisors supplement the activities of the Call Center Manager in developing and maintaining an organizational climate that facilitates attainment of the goals and objectives of the Call Center Project. This position is responsible for assigning work among CSRs, monitoring day-to-day operations, creating performance reports, enforcing company policy, and assisting with the complaint process. This position's primary responsibilities include ensuring optimal productivity in providing accurate and consistent information, as well as first class customer service to customers. The Supervisor will report all activities, trends, and concerns (and recommended solutions, as appropriate) to the Call Center Manager. Supervisors oversee Lead CSRs and CSRs.

Lead Customer Service Representatives

Lead CSRs will assist and provide oversight for the Supervisor in the day-to-day operations of the Call Center Project by providing leadership and "on-the-floor" support and mentoring to



CSRs. This position participates in on-the-job training for the CSRs in conjunction with the Supervisor. This position coordinates with the Supervisor on the required training and follow-up of staff based on quality assurance monitoring results. The Lead CSR works closely with the Supervisor to support and assist the CSRs by handling escalated interactions and complaints for follow-up and/or resolution while assuring that the CSRs appropriately process interactions. This position will perform all the duties of the CSR while also mentoring less experienced CSRs and maintaining high quality customer service standards (i.e., treats and handles all calls with respect and dignity, listens carefully, maintains confidentiality, and provides education).

Customer Service Representatives (CSR)

CSRs are responsible for providing accurate and consistent information to callers. CSRs use the tools available in the omnichannel and CRM systems (including scripting and knowledgebase resources) to accurately respond to all omnichannel interactions. The CSRs access tools and log all complete work in the CRM. The CSR provides for necessary translation assistance at the time of call, including TDD or TYY for callers with speech/hearing impairments and Language Line Translation services for non-English-speaking callers.

f. Employee Engagement

Retaining talented staff results in decreased turnover costs and, more importantly, better customer service delivery and an enhanced ability to respond to changing Project needs. Our overall retention approach results in high rates of retention, enhanced customer service, and improved morale (Exhibit 7). Within the overall retention framework, we pay close attention to several factors and analyze attendance and performance data to identify when an employee may be preparing to exit. For example, employees with dips in quality or productivity scores may be dissatisfied and preparing to leave. We couple the performance and productivity monitoring with assessing attendance and time on the phones for unexpected and increased absences, which are also signs of employee dissatisfaction.

Did You Know?

Many of our projects conduct annual in-person events, such as company provided tickets to baseball games and annual holiday parties. Examples of other activities we have performed include lunch and learn sessions with local organizations (e.g., H&R Block, AAA, etc.) and donations for local organizations (e.g., local humane society and veterans' associations, etc.).



Exhibit 7. Approach to Employee Engagement

	Employee Selection	<ul style="list-style-type: none"> Recruit staff with appropriate skills, education, and relevant background Value enthusiasm, passion, and commitment to serve the Project
	Training Plans	<ul style="list-style-type: none"> Provide clear expectations for job performance, skills, and knowledge needed Conduct ongoing training to keep skill levels high and staff engaged in performance
	Career Paths	<ul style="list-style-type: none"> Develop and retain top performing talent Provide leadership training to further hone skills and engage staff
	Mentorship Program	<ul style="list-style-type: none"> Mentors meet regularly to discuss issues that impact the workplace and Managers Goals are to help employees develop skills for the next level of management
	Corporate Culture	<ul style="list-style-type: none"> Employees are valued, treated fairly, and rewarded for excellent performance Modern amenities and technology are provided to demonstrate commitment to quality
	Benefits	<ul style="list-style-type: none"> Comprehensive benefits packages at multiple levels to accommodate various needs Benefits are supplemented by a free Corporate Wellness Program
	'People Group'	<ul style="list-style-type: none"> Ensures Project Leadership listens and is responsive to the needs of employees Implements employee recognition/incentives and coordinates holiday functions <p><i>Our comprehensive approach to retention maximizes performance.</i></p>

Our Supervisors and Managers are acutely aware of the benefits of retention and are invested in supporting our goals. All Supervisors provide one-on-one meetings with staff, and our Management Team engages in ongoing communication with all Project employees. Our Supervisors engage in a friendly and informal competition with each other to see who can achieve the highest team retention rate. We also invest in specific strategies that are unique to the needs of each Project. For example, in our Rhode Island Exchange Contact Center Project, the intensity of open enrollment places significant stress on our staff. We provide financial incentives to staff who successfully complete each open enrollment period. Depending on the Project needs, we also consider incentives in quality scores and attendance.

Florida Call Center Retention Case Study

In support of a significant expansion in our Florida Project, we were responsible for recruiting and hiring more than 200 staff to accommodate the peak months of the rollout. We recognized the challenges associated with hiring and training such a large volume of staff and incorporated several onboarding strategies to maximize retention and employee success:

- **Strategic Recruitment:** We specifically recruited staff who could respond to high-volume demands.
- **Reminders:** We used many notifications to alert staff of the protocols for their first day on the job. These protocols were successful – we experienced a no-show rate of less than 1%.
- **High-Profile Welcomes:** We included welcome and introductions from our Project Director and the State Bureau Chief and invited guests from our client, which inspired staff and stressed employees' importance and roles in making such a critical initiative successful.
- **Ongoing Training Strategies:** The challenges associated with training a large volume of CSRs may adversely impact retention and performance. We incorporated a series of

Did You Know?

"AHS has been a trusted partner to Florida's Agency for Healthcare Administration. AHS executed one of the largest Medicaid Managed Care program implementations on time while staying responsive to AHCA's evolving Member and process needs."

– Ms. Liz Dudek,
Former Secretary for AHCA



games, quizzes, and creative training strategies to keep staff engaged. We immediately incorporated on-the-job training once staff completed the initial training and were accepting calls. These on-the-job scenarios reinforced critical knowledge and kept staff engaged, motivated, and equipped with essential skills throughout their performance.

- **Ongoing Communication:** Our Management Team engaged in extensive communication with our team. They relayed compliments from our client and the stakeholder community, commended staff on their commitment, and celebrated performance success.

Not only were our retention rates outstanding, but our performance reflected this ongoing commitment—despite an intense and complicated rollout, we did not miss a single SLA during the SMMC implementation, even when call volumes exceeded 250,000 calls per month. Our quarterly turnover ranged from 3-20%, well below the industry average of 40%.⁵

Did You Know?

"The Florida Hospital Association commends the Agency for Health Care Administration on its commitment to ensuring the successful implementation of the roll-out of Statewide Medicaid Managed Care. We look forward to the continued partnership to provide the highest quality care to our patients and communities."

– Bruce Rueben, Former President, Florida Hospital Association

ii. VPAT

A VPAT is not applicable to this bid.

iii. Security Certification and Accreditation

Our Security Certification and Accreditation is provided following this page.

⁵ <https://www.avoxi.com/blog/call-center-attribution-turnover-rates/>



iv. Service Level Agreements

In all our Projects, we are responsible for meeting or exceeding numerous performance standards to ensure we represent our clients with quality service. We have established tools and protocols to meet all performance standards. These tools are scalable and have allowed us to meet fluctuating call volumes without compromising SLAs.

We have extensive experience adhering to all SLAs for a variety of contracts with requirements similar to those of the RFP. Our proposed SLAs and approaches to meet them follow.

Abandoned Call Rate Must Not Be in Excess of 7%

We propose a monthly abandonment rate of less than or equal to 7%. We have successfully maintained standards for abandonment rates in all our Projects. For example, in our TennCare Connect Project, our abandonment rate for May 2022 was 0%.

Our approach to meeting the proposed abandonment rate standard of less than 7% is based on the components detailed in Exhibit 8.

Exhibit 8. Steps to Meet Abandonment Rate SLAs

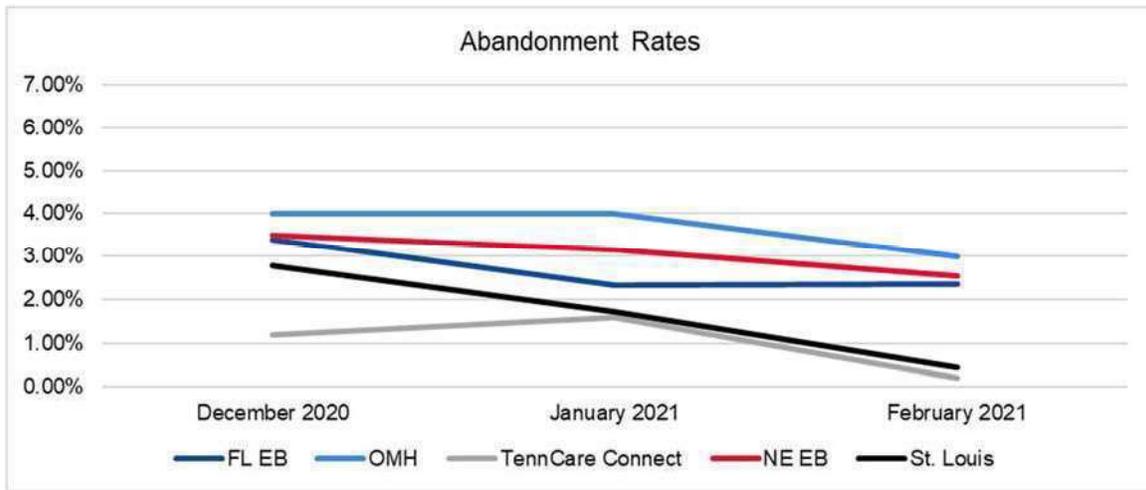
Step	Description
Staffing Model	<ul style="list-style-type: none"> Flexible staffing model, consisting of a complement of part-time staff whose hours can be adjusted during periods of increasing call volume Refined based on ongoing workforce analytics
Scheduling	<ul style="list-style-type: none"> Staff schedules based on call volumes to ensure coverage for all hours Protocols for time off so that ample staff are always available on the phones Adjust staff schedules throughout the day (e.g., suspend time away from the phones for meetings or trainings)
ACD	<ul style="list-style-type: none"> Call routing (e.g., oldest call has priority) to minimize wait times Skills-based routing based on rules-driven logic to ensure all calls are directed to a CSR with the most appropriate skills Prompts in English and Spanish
Monitoring and Reporting	<ul style="list-style-type: none"> Real-time monitoring so the Management Team can adjust as needed, such as canceling all time away from the phones Historical monitoring to coordinate schedules appropriately Time-to-abandon monitoring

Our strategies for meeting abandonment rates are proven to exceed targets for the Call Center Project.

Examples from some of our contracts that demonstrate the success of these methods are provided in Exhibit 9. All rates are far under contractual performance metrics.



Exhibit 9. Abandonment Rates



Our methods have been proven successful.

60 Seconds or Less for the Average Speed to Answer (ASA)

We propose an ASA of 60 seconds or less. We use four components to ensure the ASA is less than 60 seconds:

- **Flexible Staff Model:** We utilize a complement of part-time CSRs, and we can adjust their hours to ensure ample staff are available to answer the calls promptly.
- **Track Statistics:** Average speed to answer is a key statistic we track in real time throughout the day. We also track the maximum time in queue throughout the day.
- **Queue Monitoring:** Supervisors monitor the queues on an ongoing basis. Immediately upon identifying that any metric, including average speed to answer, is not optimal, they implement appropriate steps to correct the issue before it escalates into additional problems. These steps may include such measures as suspending time away from the phones (e.g., for trainings, meetings), reassigning bilingual staff to another queue, etc.
- **Workforce Analytics:** We use ongoing workforce analytics to continuously evaluate the number of staff needed for operations. We refine all projects on a daily, weekly, and monthly basis for maximum accuracy, performance, and service.

We hold ourselves accountable for superior performance and are proud of our established record of impressive performance statistics, including prompt answering.

Two Minutes or Less for Average Hold Time

We propose a monthly hold time of 2 minutes or less. Our policies and procedures require staff to ask permission prior to placing any caller on hold. If a CSR must place a caller on hold and the hold time is longer than 90 seconds, we ask CSRs to check in with the caller to let them know that we will be with them shortly.

Satisfaction Rate of 85% or Higher

We propose a monthly satisfaction rate, as assessed by satisfaction surveys, of 85% or higher. Our multiple strategies that ensure high performance have been successfully proven to earn satisfaction survey scores of 90% or more in several contracts. These strategies include:

- OMES-approved scripting that is embedded in our CRM



- OMES-approved policies and procedures that underlie all workflows, ensuring work is performed in a manner that reflects OMES standards
- Initial and ongoing training regarding customer service, sensitivity, and operational workflows
- Quality improvement plan to monitor and target performance

Occupancy Rate 80% or Higher

We propose a monthly occupancy rate of 80% or higher. We use multiple standards to meet occupancy rate standards:

- Supervisors are tracked with monitoring occupancy rate on an ongoing basis and make needed adjustments throughout the day.
- Supervisors are notified of outliers in occupancy rate performance and provide ongoing support and troubleshooting.
- Staff schedules are developed in conjunction with workforce management analytics and are closely tied to anticipated call center volumes.

Sample Performance Report

A sample performance metrics report from our call center contract for the State of Nebraska is provided in Exhibit 10.

Exhibit 10. Performance Metrics Report

Heritage Health Enrollment Broker SLA Report - February 2021

Performance Measure	Requirement	Achieved Metric	Over/Under Requirement	Measure	Penalty	Total Penalty Amt	Requesting Waiver (Yes/No)	Comments
Abandonment Rate (5% or less)	5%	2.55%	-3%	Per Percent (rounded up) above 5%	\$ 500.00	\$ -	No	
Blocked Call Rate (1% or less)	1	NA	NA	Per Percent (rounded up) above 1%	\$ 1,000.00	\$ -	No	All B does not block calls. Therefore, this metric will always be 0%.
Average Hold Time (30 seconds or less)	0:00:30	0:00:06	-1	Per 5 Seconds (rounded up) above 30 seconds average hold	\$ 500.00	\$ -	No	
Average Wait Time (2 minutes or less)	0:02:00	0:00:34	-1	Per Minute (rounded up) above 2 minutes	\$ 500.00	\$ -	No	
System Readiness	0	0	0	Per Calendar Day late	\$ 5,000.00	\$ -	No	
Operational Readiness	0	0	0	Per Calendar Day late	\$ 5,000.00	\$ -	No	
Initial Enrollment Period	9/1/2016	9/1/2016	0	Per Calendar Day late	\$ 10,000.00	\$ -	No	
Key Staff	30	0	-30	Per Calendar Day late	\$ 1,000.00	\$ -	No	
Reports and Data	0	0	0	Per Calendar Day late	\$ 1,000.00	\$ -	No	
Interface Files	0	0	0	Per Calendar Day late	\$ 500.00	\$ -	No	
MCO Provider Files	0	0	0	Per Hour (rounded up) of delay	\$ 100.00	\$ -	No	
Recipient Enrollment Database	0	0	0	Per Hour (rounded up) of delay	\$ 100.00	\$ -	No	
Enrollment Information	0	0	0	Per Calendar Day a member's MCO enrollment is delayed	\$ 1,000.00	\$ -	No	
Returned Calls	0	0	0	Per Occurrence	\$ 100.00	\$ -	No	
Welcome Packet for New Members	0	0	0	Per Occurrence	\$ 500.00	\$ -	No	
Website Uptime	99%	99.86%	-1.00%	Per Percent (rounded up) below 99%	\$ 2,500.00	\$ -	No	
Restoration of Operations	72	0	-72	Per Hour (rounded up) in excess of 72 hours	\$ 1,000.00	\$ -	No	
Turnover Plan	0	0	0	Per Calendar Day (rounded up) late, inaccurate, or incomplete	\$ 5,000.00	\$ -	No	
Ad hoc Reports	5	0	5	Per Calendar Day (rounded up) late, inaccurate, or incomplete	\$ 1,000.00	\$ -	No	
MCO Steering	0	0	0	Per Member	\$ 5,000.00	\$ -	No	
TOTAL						\$ -		

We provide regular reporting, both internally and to our clients, on performance against metrics of performance.

Matrix for Service Credits

Our matrix for service credits is provided in Exhibit 11 as measured on a monthly basis.

Exhibit 11. Matrix for Service Credits

Standard	Monthly Credit
Abandonment rate	1% of our monthly invoice for failure to meet the abandonment rate standard
ASA	1% of our monthly invoice for failure to meet the ASA standard



Standard	Monthly Credit
Hold time	1% of our monthly invoice for failure to meet the hold standard
Satisfaction rate	1% of our monthly invoice for failure to meet the satisfaction rate standard
Occupancy rate	1% of our monthly invoice for failure to meet the occupancy rate standard

We have assigned service credits for failure to meet proposed SLAs.

v. Statement of Work

AHS must perform all the requirements of the Scope of Work outlined below. The core services requested by OMES must consist of the following:

- Account Management
- Implementation
- Information Security
- Training Requirements
- Readiness Review
- Call Center Operations
- System and Infrastructure Requirements
- Reporting Requirements
- Disengagement Plan

Account Management

AHS will:

- Provide and maintain qualified personnel and staffing to enable the deliverables to be provided in accordance with the contract.
- Ensure that all persons assigned to perform work under the contract are employees and are fully qualified to perform the services required.
- Notwithstanding the above provisions, AHS may terminate any of its employees designated to perform work or services under this contract, as permitted by applicable law.
- In the event of an AHS employee termination, provide OMES with immediate notice of the termination, the reason(s) for the termination if it adversely impacts the contract (e.g., breach, embezzlement, or fraud) and an action plan for replacing the discharged employee.
- Have a single point of contact for OMES with overall responsibility for AHS' functions under the contract. The contact person will have the authority to make decisions and resolve problems on behalf of AHS with OMES.

Implementation

AHS will:

- Propose an implementation plan that is logical in its sequence of events, including appropriate review time by OMES and sufficient detail for review.
- Develop and maintain electronic versions of operating policy and procedure manuals for each function identified in the Scope of Work.
- Submit a weekly progress written report to OMES during the implementation phase.
- Operate the Call Center within the Continental U.S.



- Provide computers and all other equipment necessary for secure Internet email access with OMES staff.
- Launch operations following approval from OMES.

Information Security

AHS will meet all OMES required information security requirements.

Readiness Review

OMES will:

- Conduct a readiness review of AHS.
- Provide program policy clarification when requested by AHS.

Call Center Operations

AHS will:

- Operate and maintain technical capability (i.e., computer equipment, databases, phones and appropriate communications infrastructure, Internet access and staffing) to provide Call Center services on behalf of OMES:
 - Add and/or update caller information on clients in OMES' client information systems, as directed by OMES.
 - Provide live outbound calls as needed, recording all, and including an initial message that the call is being recorded.
 - Communicate with OMES' liaison for call-related problem resolution.
 - Conduct satisfaction surveys following a set number of calls as directed by OMES.
 - Adhere to OMES' approved policies and procedures and scripting when performing call center services.

Quality Monitoring

AHS will:

- Provide OMES with the ability to monitor live and recorded calls for quality assurance.
- Record and retain inbound and outbound live calls per OMES' retention policies.
- Make the recordings available to OMES upon request.
- Perform a monthly quality review of a sample of calls per CSR and assess the quality of the response provided to the caller for customer service and accuracy in accordance with the evaluation criteria mutually agreed upon by AHS and OMES.

Training/Security

AHS will:

- Develop a Training Plan that will be submitted to OMES for approval.
- Provide initial training of call center employees, to include:
 - Administer a test.
 - Ensure all trainees score 85% or higher.
 - Provide continuous up-to-date training of staff.
 - Assure most current approved materials are provided to applicable call staff.



- Require call center staff to sign required confidentiality forms before commencement of work and annually thereafter to access OMES' client information system.
- Provide documentation to OMES upon request.
- Provide quality and refresher training as specified in the OMES-approved Training Plan.
- Administer ongoing security training.

System and Infrastructure Requirements

AHS will:

- Provide a CRM to log call details (e.g., basic caller demographics, the reasons for the call, and any actions taken).
- The CRM must have sufficient capacity that ensures that infrastructure, capacity, bandwidth, and hardware or software are not limiting factors.
- Notify OMES of any disruption or irregularity in service during business hours within fifteen (15) minutes of recognition or knowledge of the problem.

Reporting Requirements

AHS will provide weekly standard reports for Call Center services:

- Reports will be generated from NICE CXone and the CRM.
- Reports generated from external systems will include call actions (e.g., actions performed by a CSR while on a call), staffing updates, and quality results.

Additional Security Requirements

AHS will:

- Log and examine system activity in accordance with industry standard audit policies and procedures.
- Provide security incident reporting and mitigation mechanisms for security incidents.
- Ensure the protection of the confidentiality and integrity of information and maintain the technical mechanisms of legitimate access to it. AHS must comply with the HIPAA security rules and any State or Federal statutes related to security.
- Schedule supervisory positions to be present for all shifts and during overtime. Supervision will be relevant to the type of work being performed.

Disengagement Plan

- AHS will ensure that program stakeholders do not experience any adverse impact from the transfer of AHS' responsibility of providing operations services to either OMES or a successor contractor.
 - Three (3) months prior to the end of the initial contract period or any extension thereof, AHS must provide an OMES-approved Disengagement Plan covering the possible turnover of the records and information maintained to either OMES or a successor contractor unless waived by OMES.
 - The Disengagement Plan must be a comprehensive document detailing the proposed schedule, activities and resource requirements associated with the turnover tasks outlined in the sections below.



- As part of the Disengagement Plan, AHS must provide OMES with copies of all relevant data and reference tables, documentation, or other pertinent information necessary to assume the operational activities successfully.