FILED IN DISTRICT COURT
OKLAHOMA COUNTY

JAN 22 2026

RICK WARREN
COURT CLERK
108 ____________

IN THE DISTRICT COURT OF OKLAHOMA COUNTY
STATE OF OKLAHOMA

THE STATE OF OKLAHOMA *ex rel.* THE OKLAHOMA ETHICS COMMISSION

Plaintiff,

v.

RFD & ASSOCIATES, INC., a foreign corporation,

Defendant.

Case No: CJ- 2026 - 558

PETITION

COMES NOW, Plaintiff, the State of Oklahoma *ex rel.* the Oklahoma Ethics Commission (the "Ethics Commission") and for its claims against Defendant, RFD & Associates, Inc. ("RFD"), states the following:

PARTIES, JURISDICTION, AND VENUE

1. Plaintiff, the Ethics Commission, is a state agency created by Article XXIX of the Oklahoma Constitution and is located in Oklahoma County, Oklahoma.

2. Defendant, RFD, is a foreign corporation and is registered to do business in the State of Oklahoma. Upon information and belief, RFD is organized under the laws of the State of Texas, with its principal place of business in Austin, Texas.

3. The acts and omission giving rise to this matter arise out of a written agreement between the Ethics Commission and RFD dated December 6, 2024 (the "Contract").

4. The Oklahoma County District Court has general jurisdiction to decide matters involving disputes between the State of Oklahoma and Defendant. Further, this Court has jurisdiction over this matter pursuant to Oklahoma's long-arm statute. 12 O.S. § 2004(F).

5. Venue is proper in this Court pursuant to Section 26.1 of the Contract.

STATEMENT OF FACTS

6. On or about June 14, 2024, the Ethics Commission began soliciting bids from providers to create and maintain a filing system where candidates, political action committees, and lobbyists could submit financial disclosures and other required reports. *See* Solicitation, attached hereto as Exhibit 1.

7. On or about December 6, 2024, the Ethics Commission entered into a written agreement with RFD, whereby RFD agreed to provide the services described in the Solicitation. *See* Contract, attached hereto as Exhibit 2.

8. On or about January 3, 2025, the parties executed a Statement of Work, setting out due dates on the following seven (7) deliverables:

a.	Project Kick-Off	Due: 12/18/24
b.	Requirements Sign-Off	Due: 2/3/25
c.	Design Sign-Off	Due: 2/24/25
d.	Start of User Acceptance Test	Due: 6/16/25
e.	Go-Live	Due: 7/1/25
f.	Data Migration	Due: 6/20/25
g.	Training	Due: 6/30/25

See Statement of Work, attached hereto as Exhibit 3 at 4.

9. RFD failed to complete six of the seven deliverables by the agreed upon deadlines set out in the Statement of Work; the only deliverable that was submitted on time was the "Project Kick-Off."

10. Throughout the project, RFD repeatedly provided system-ready assurances despite known deficiencies, forcing the Ethics Commission to issue public delay notices, extend deadlines for filers, and field daily inquiries from legislators, candidates, PACs, lobbyists, political subdivisions, the media, and the public.

11. In late June of 2025, after it became clear that RFD would fail to meet the July 1, 2025 "Go-

Live" deadline, the Ethics Commission entered into a contract with a third party to extend the outgoing campaign finance filing and disclosure system, (the "Guardian"), for an additional 3 months.

12. At that time, RFD represented to the Ethics Commission that its system would be operational by September 1, 2025.

13. On August 18, 2025, the Ethics Commission contacted RFD's CEO to express their grave concerns about RFD's repeated failure to meet contractual deadlines.

14. On August 25, 2025, the parties executed an Amendment to their Contract, whereby they agreed that payment would be delayed on certain deliverables until all deliverables were completed. *See* Amendment, attached hereto as Exhibit 4. Despite the renewed promises, RFD continued missing deadlines and deliverables.

15. On November 25, 2025, the Executive Director of the Ethics Commission wrote a letter to RFD, outlining RFD's failure to meet contractual deadlines and demanding that RFD take immediate corrective action.

16. On or about December 19, 2025, after RFD failed to take appropriate corrective action, the Ethics Commission terminated the Contract for cause.

CAUSE OF ACTION I: BREACH OF CONTRACT

17. The Ethics Commission hereby reincorporates and re-alleges each of the paragraphs above, as though fully set forth herein.

18. The Ethics Commission and RFD entered into the Contract on or about December 6, 2024. From and since that time, RFD failed to meet contractual deadlines. Moreover, with its failure to meet the contractual deadlines and deliverables, RFD continuously and repeatedly assured the Ethics Commission that it would rectify the errors and deliver a fully operational system, including by July 1, 2025, September 1, 2025, October 1, 2025, October 28, 2025, and December 16, 2025. In each instance, RFD fails to meet the deadlines.

19. RFD's failure to meet contractual deadlines constitutes a material breach of the Contract.

20. RFD's failure to provide the Ethics Commission with an operational system is a material breach of the Contract.

21. RFD's failure to provide the Ethics Commission with the system described and contracted for prevented and impeded the Ethics Commission from performing its constitutional and statutory duties.

22. The Ethics Commission has been damaged as a direct result of RFD's material breaches.

23. The Ethics Commission is continuing to evaluate its damages. At the present time, the Ethics Commission estimates that it has suffered damages in excess of $800,000 as a direct result of RFD's breaches.

CAUSE OF ACTION II: UNJUST ENRICHMENT

24. The Ethics Commission hereby reincorporates and re-alleges each of the paragraphs above, as though fully set forth herein.

25. The Ethics Commission paid RFD an amount in excess of $800,000 to provide a campaign finance filing and disclosure system.

26. RFD has failed to provide an operational campaign finance filing and disclosure system to the Ethics Commission.

27. RFD continues to retain the funds paid to it by the Ethics Commission and it would be unjust to allow RFD to retain such funds.

28. The Ethics Commission is continuing to evaluate its damages. At the present time, the Ethics Commission estimates that it has suffered damages in excess of $800,000 as a direct result of RFD's unjust enrichment.

CAUSE OF ACTION III: FRAUD

29. The Ethics Commission hereby reincorporates and re-alleges each of the paragraphs above, as though fully set forth herein.

30. Throughout bidding process, RFD represented to the Ethics Commission that it was capable of providing a functional campaign finance filing and disclosure system.

31. On or about January 23, 2025, RFD represented to the Ethics Commission that the system would be operational on July 1, 2025.

32. After January 23, 2025, RFD repeatedly represented to the Ethics Commission that it would meet agreed upon deadlines.

33. Each of the above representations by RFD was a material misrepresentation made as a positive assertion to the Ethics Commission.

34. RFD knew that each of the above material representations were false.

35. RFD intended the Ethics Commission to rely on its material misrepresentations.

36. The Ethics Commission, to its detriment, relied on RFD's misrepresentations.

37. The Ethics Commission is continuing to evaluate its damages. At the present time, the Ethics Commission estimates that it has suffered damages in excess of $800,000 as a direct result of RFD's fraud.

<u>Cause of Action IV: Breach of Express Warranties</u>

38. The Ethics Commission hereby reincorporates and re-alleges each of the paragraphs above, as though fully set forth herein.

39. In the Contract, RFD expressly warranted that its services would be "performed in accordance with industry best practices." Ex. 2 at 7.

40. In the Contract, RFD expressly warranted that its deliverables would "be substantially uninterrupted and error-free in operation." *Id.*

41. RFD breached these express warranties when it failed to provide the Ethics Commission with a functional campaign finance filing and disclosure system.

42. The Ethics Commission is continuing to evaluate its damages, and at the present time, the Ethics

Commission estimates that it has suffered damages in excess of $800,000 as a direct result of RFD's breach of express warranties.

Cause of Action V: Breach of Implied Warranties

43. The Ethics Commission hereby reincorporates and re-alleges each of the paragraphs above, as though fully set forth herein.

44. RFD is in the business of providing campaign finance filing and disclosure system.

45. RFD represented to the Ethics Commission that it could provide the systems and services described in the Ethics Commissions' Solicitation.

46. RFD breached the implied warranty of merchantability when it failed to provide the Ethics Commission with a functional campaign finance filing and disclosure system.

47. RFD breached the implied warranty of fitness for particular purpose when it failed to provide the Ethics Commission with a functional campaign finance filing and disclosure system.

48. The Ethics Commission has been damaged as a direct result of RFD's breach of the implied warranties of merchantability and fitness for particular purpose.

49. The Ethics Commission is continuing to evaluate its damages, and at the present time, the Ethics Commission estimates that it has suffered damages in excess of $800,000 as a direct result of RFD's breach of the implied warranties.

Cause of Action VI: Negligent Misrepresentation

50. The Ethics Commission hereby reincorporates and re-alleges each of the paragraphs above, as though fully set forth herein.

51. RFD represented to the State in the course of its business to design, build, and deliver the Guardian 2.0 system, as described and detailed in the Contract.

52. Through its response to the Solicitation, executing the Contract, the Amendment, and ongoing representations through the Ethics Commission terminating the Contract, RFD represented that it had

the necessary experience, skill, and team, for the Ethics Commission's campaign finance filing and disclosure system, as described and detailed in the Contract.

53. RFD also made representations that it would provide certain functionalities and deliverables within established deadlines in the Contract.

54. RFD supplied false information to the Ethics Commission. First and foremost, RFD misrepresented its experience and capabilities to develop and deliver the Ethics Commission's campaign finance filing and disclosure system. Second, RFD provided false information when it detailed which functionalities would be fully operational and delivered under the deadlines established in the Contract. Third, RFD admitted that it overpromised and underdelivered, and that it withheld timely communication of its inability to deliver. Further, RFD supplied false information when it promised to complete and deliver a fully operational system under the deadlines and terms established in, and after, the Amendment.

55. RFD did not exercise or use reasonable care or competence in obtaining or communicating the information.

56. The Ethics Commission justifiably relied on the representations.

57. RFD's negligence representations caused the Ethics Commission injury in at least the amount of $800,000.

Cause of Action VII: Violation of the Oklahoma Deceptive Trade Practices Act

58. The Ethics Commission hereby reincorporates and re-alleges each of the paragraphs above, as though fully set forth herein.

59. RFD's violations under the Oklahoma Deceptive Trade Practices Act ("ODTPA") are numerous and avail the Ethics Commission of all remedies provided by the ODTPA.

60. RFD is a person as that term is defined under 78 O.S. § 52 and who can be sued under the ODTPA.

61. RFD's violations under the ODTPA include such things as representing that it possessed the skill, experience, time, and other necessary capabilities to deliver the Ethics Commission's campaign finance filing and disclosure system, as detailed in the Solicitation and the Contract.

62. RFD also made false representations relating to the approval and certification, the characteristics, benefits and uses, status of the quantities and approvals in relation to the products and services detailed in the Contract.

63. RFD admitted that it overpromised and underdelivered, and that it withheld timely communication of its inability to deliver.

64. RFD failed to develop and deliver the Ethics Commission's campaign finance filing and disclosure system with the functionalities outlined in the Contract.

65. RFD's actions were a producing cause of the Ethics Commission's damages.

66. RFD's violations under the ODTPA caused the Ethics Commission injury in at least the amount of $800,000.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, the State of Oklahoma *ex rel.* the Oklahoma Ethics Commission respectfully requests that this Court enter judgment in Plaintiff's favor on each of its causes of action against Defendant, RFD & Associates, Inc., and award Plaintiff damages in an amount in excess of $800,000 and all costs and expenses associated with the prosecution of this action, as well as any other relief this Court deems just and proper.

Respectfully submitted,

GARRY M. GASKINS, II, OBA #20212
Solicitor General
SAM BLACK, OBA #34614
Assistant Solicitor General

OFFICE OF THE ATTORNEY GENERAL
STATE OF OKLAHOMA
313 N.E. 21st Street
Oklahoma City, OK 73105
Main: (405) 521-3921
Garry.Gaskins@oag.ok.gov
Samuel.Black@oag.ok.gov

Counsel for Plaintiff

CERTIFICATE OF SERVICE

I hereby certify that on the 22nd day of January 2026, a true and correct copy of the foregoing document was mailed, postage pre-paid to the following:

RDF & Associates, Inc.
3267 Bee Caves Rd, Ste 107-61
Austin, TX 78746

GARRY M. GASKINS, II, OBA #20212

ATTACHMENT A

SOLICITATION/EVENT NO. EV00000504

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

PURPOSE

The Contract is awarded on behalf of the Oklahoma Ethics Commission for Suppliers, and their partners to supply a Political Finance software solution to The Oklahoma Ethics Commission for the benefit of The State of Oklahoma.

BACKGROUND

The Guardian System replacement project is driven by the urgent need to modernize the state's approach to political finance transparency and accountability. The primary motivation behind this project is to ensure the continuation of efficient and secure data processing and reporting as the current system approaches its End of Life (EOL) and End of Service in June 2025. The project aims to enhance scalability and performance, improve user experience, ensure compliance and security, enable integration, and streamline maintenance and support.

1. Contract Term and Renewal Options

The initial Contract term, which begins on the effective date of the Contract, is one year subject to the state's option to terminate early. After the initial 1-year term, there will be four (4) one-year options to renew.

2. Solicitation Criterion

The Bid will be evaluated using a best value criterion, based on the following:

I. Technical Requirements
II. Cost
III. References

3. Scope and Description

EXHIBIT
1

Certain Contract requirements and terms are attached hereto as Exhibit 1 Specifications and incorporated herein.

OKLAHOMA
Office of Management
& Enterprise Services

State of Oklahoma
Office of Management and Enterprise Services

STATE OF OKLAHOMA CONTRACT WITH RFD & ASSOCIATES, INC.

This State of Oklahoma Contract ("Contract") is entered into between the State of Oklahoma by and through the Oklahoma Ethics Commission ("State") and RFD & Associates, 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 to this Contract. The initial term of the Contract shall be for 1 year with four (4) one-year options to renew.

Purpose

The State is awarding this Contract to Supplier for the provision to supply a Political Finance software solution to The Oklahoma Ethics Commission for the benefit of The State of Oklahoma, as more particularly described in certain Contract Documents. This Contract 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 this Contract. 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 #EV00000504, Attachment A;
   2.2. General Terms, Attachment B;
   2.3. Intentionally Omitted, Attachment C;
   2.4. Information Technology terms, Attachment D;
   2.5. Exhibit 1 Response to Specifications, Attachment E;
   2.6. Pricing, Attachment E-1;
   2.7. Support Services and Service Level Agreement, Attachment E-2; and
   2.8. Negotiated Exceptions to Contract, Attachment F.

3. The parties additionally agree:

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

   3.3. In lieu of direct payment and as fair and reasonable consideration, State agrees to accept the discounted amount, in Attachment E-1, as compensation in exchange for the state granting Supplier joint ownership of the intellectual property in the work product related to this Contract.

EXHIBIT
2

3.4. Supplier shall deposit the source code for the work product into a secure repository and escrow account designated by the State. The repository or escrow documentation shall explicitly name the State as an owner of all intellectual property rights in the source code, with full rights to use, modify, and distribute the source code without restriction. The supplier shall ensure that source code is complete, up to date, and accessible by the State upon request or as otherwise required by this agreement. For clarity, nothing herein shall require the supplier to update or support the software after the termination of this agreement unless otherwise agreed to by the parties in writing.

3.5. The parties shall develop the SOW to include data migration, obligations, timelines, outages, technical needs, resources, etc. and amend this Contract with the updated SOW along with Service Level Agreements ("SLAs") as necessary.

3.6. 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.

3.7. This Contract is expressly contingent upon Supplier obtaining the specified insurance coverage as outlined in Attachment B Section 8.1(D) of this Contract prior to any IT services performed.

4. Payment obligations rest solely with the Oklahoma Ethics Commission

Please send invoices and billing inquiries to:
2300 N Lincoln Blvd, Room G-27, Oklahoma City, Oklahoma 73105, United States
Darci.Ray@ethics.ok.gov

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

5. 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.

6. The undersigned Agency hereby attests that any required terms and conditions based on a Federal Award applicable to this Contract are included herein.

SIGNATURES

The undersigned represent and warrant that they are authorized, as representatives of the party on whose behalf they are signing, to sign this Contract and to bind their respective party thereto.

STATE OF OKLAHOMA **by and through the OKLAHOMA ETHICS COMMISSION**	**RFD & ASSOCIATES, INC.**
By: Lee Anne Bruce Boone Lee Anne Bruce Boone (Dec 5, 2024 17:27 CST)	By: Scott T. Glover Scott T. Glover (Dec 5, 2024 13:52 CST)
Name: Lee Anne Bruce Boone	Name: Scott T. Glover
Title: Executive Director	Title: COO
Date: 12/05/2024	Date: 12/05/2024

The Chief Information Officer is signing solely to approve the Contract pursuant to 62 O.S., § 34.11.1 concerning procurement of Information Technology and/or Telecommunications.

By: Aleta Seaman
Aleta Seaman (Dec 6, 2024 08:10 CST)

Name: Aleta Seaman

Title: Interim CIO

Date: 12/06/2024

ATTACHMENT A

SOLICITATION/EVENT NO. EV00000504

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

PURPOSE

The Contract is awarded on behalf of the Oklahoma Ethics Commission for Suppliers, and their partners to supply a Political Finance software solution to The Oklahoma Ethics Commission for the benefit of The State of Oklahoma.

BACKGROUND

The Guardian System replacement project is driven by the urgent need to modernize the state's approach to political finance transparency and accountability. The primary motivation behind this project is to ensure the continuation of efficient and secure data processing and reporting as the current system approaches its End of Life (EOL) and End of Service in June 2025. The project aims to enhance scalability and performance, improve user experience, ensure compliance and security, enable integration, and streamline maintenance and support.

1. Contract Term and Renewal Options

The initial Contract term, which begins on the effective date of the Contract, is one year subject to the state's option to terminate early. After the initial 1-year term, there will be four (4) one-year options to renew.

2. Solicitation Criterion

The Bid will be evaluated using a best value criterion, based on the following:

I. Technical Requirements
II. Cost
III. References

3. Scope and Description

Certain Contract requirements and terms are attached hereto as Exhibit 1 Specifications and incorporated herein.

ATTACHMENT B

STATE OF OKLAHOMA GENERAL TERMS

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

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 Amendment. 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 Amendment;

B. terms contained in this Contract document

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

D. any applicable Solicitation;

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 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 Amendment.

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 Amendment. 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.

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

3.4 Unless mutually agreed to in writing by the State of Oklahoma by and through the Office of Management and Enterprise Services, no Contract document or other terms and conditions or clauses, including via a hyperlink or uniform resource locator, shall supersede or conflict with the terms of this Contract or expand the State's or Customer's liability or reduce the rights of Customer or the State. If Supplier is acting as a reseller, any third-party terms provided are also subject to the foregoing.

3.5 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 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 **Amendment** means a mutually executed, written modification to a Contract document.

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

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

4.5 **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.

4.6 **Customer** means the governmental entity rece1vmg goods or services contemplated by the Contract.

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

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

4.9 **Governmental Entity** means any governmental entity specified as a political subdivision of the State pursuant to the Governmental Tort Claim Act including any associated institution, instrumentality, board, commission, committee, department, or other entity designated to act on behalf of the state.

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

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

4.12 **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.

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

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

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

4.16 **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.

4.17 **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.

4.18 **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.

4.19 **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.

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

5 Pricing

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

5.2 Pursuant to 74 0. 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 260:115-9-1, 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 notice of cancellation and includes 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 m 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 $2,000,000 per occurrence;

C. Automobile Liability Insurance with limits of liability of not less than $2,000,000 combined single limit each accident;

D. If the Supplier will access, process, or store state data, then 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

E. 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 Supplier's 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, Supplier's 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 2 C.F.R. part 376 in connection with Debarment, Suspension and other responsibility matters;

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

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

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

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

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

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

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

9.2 The Supplier's employees, agents and subcontractors shall adhere to applicable Customer policies including, but not limited to acceptable use of Internet and electronic mail, facility and data security, press releases, and public relations.

As applicable, the Supplier shall adhere to the State Information Security Policy, Procedures, Guidelines set forth at http://www.dhs.gov/E-Verify. 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's 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 Contract.

11.8 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 the Supplier.

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 ofits 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 13.1 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 service.

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 State Shall Not Indemnify

The State of Oklahoma cannot lawfully agree to indemnify a private contractor. The credit of the State shall not be given, pledged, or loaned to any individual, company, corporation, or association, municipality, or political subdivision of the State pursuant to Oklahoma Constitution article 10, Section 15, OAC 260:115-7-32(k)(3)(A) and Attorney General Opinion 2012-18.

16.2 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.

16.3 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.

16.4 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.

16.5 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.

16.6 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 Contract or 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 The State may terminate the Contract if the scope includes PR Vendor services and the Supplier, or Supplier's employee, violate the lobbying clause. PR Vendor services is defined to include a contract for public relations (PR), marketing or communication services. The State may immediately terminate the Contract with no more than 10-day notice under this section.

18.4 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.

18.5 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 260:115-9-1 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 nor 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., Second Floor
Oklahoma City, Oklahoma 73105

With a copy, which shall not constitute notice, to:
Purchasing Division Deputy General Counsel
2401 N. Lincoln Blvd., Second Floor
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. §85.7(F), 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. The State expressly declines any terms that minimize its rights under Oklahoma law, including but not limited to, Statutes of Limitations.

26.2 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.

26.3 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.

26.4 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.

26.5 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. 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) pricing 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.

26.6 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.

26.7 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.

26.8 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.

26.9 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.

26.10 Section Headings

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

26.11 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.

26.12 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.

26.13 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.

26.14 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.

26.15 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 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 ("The Act" or "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 **Customer Data** means all data supplied by or on behalf of a Customer in connection with the Contract, excluding any confidential information of Supplier. Customer Data includes both Non-Public Data and Personal Data.

1.2 **Data Breach** means the unauthorized access or the reasonable suspicion of unauthorized access, by an unauthorized person that results in the use, destruction, loss, alteration, disclosure, or theft of Customer Data.

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

1.4 **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.

1.5 **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.

1.6 **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.

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

1.8 **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. A Supplier with whom the State enters into an awarded Contract shall also be known as a Contractor.

1.9 **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.

1.10 **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.

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).

2.3 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

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

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

4 MEDIA OWNERSHIP (Disk Drive and/or Memory Chip Ownership)

4.1 Any disk drives and memory cards purchased with or included for use in leased or purchased products under the Contract remain the sole and exclusive 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

Standards, policies, procedures and architectures as set forth at https://oklahoma.gov/omes/services/information-services.html or as otherwise provided by the State.

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.

7 EMERGING TECHNOLOGIES

The State 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 Chief Information Officer reserves the right to extend any Contract at his or her sole option if the State Chief Information Officer determine 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 OR SUPPLIER TERMS

If Supplier specifies terms and conditions or clauses in an electronic license, subscription, maintenance, support or similar agreement, including via a hyperlink or uniform resource locator address to a site on the internet, 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. Further, no such terms and conditions or clauses shall expand the State's or Customer's liability or reduce the rights of Customer or the State.

11 OWNERSHIP RIGHTS

Any software developed, modified, or customized by the Supplier in accordance with a mutually negotiated statement of work pursuant to this 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. The parties mutually agree the State as a licensee of the Supplier does not make a claim of ownership to the existing Intellectual Property of Supplier. 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 when made in accordance with a mutually negotiated statement of work pursuant to this Contract. 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 TO WORK PRODUCT

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

12.1 As to the Intellectual Property Rights to Work Product between Supplier and Customer, Customer shall be the exclusive owner 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 agrees that all right, title and interest in and to all ownership rights and all Intellectual Property Rights in the Work Product is 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

A Supplier shall be responsible for the obligations set forth in in this Contract, including those obligations related to breach reporting and associated costs when a Supplier Hosting Customer Data or providing products or services pursuant to an Acquisition, contributes to, or directly causes a Data Breach or a Security Incident. Likewise, Supplier shall be responsible for the obligations set forth in in this Contract, including those obligations related to breach reporting and associated costs when a Supplier's affiliate or subcontractor contributes to, or directly causes a Data Breach or a Security Incident.

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 OWNERSHIP OF IT AND TELECOMMUNICATION ASSETS

Notwithstanding any other provision in the Contract and pursuant to the Oklahoma Information Technology Consolidation and Coordination Act, all information technology and telecommunication assets and contracts on behalf of appropriated agencies of the State belong to OMES-IS. OMES-IS 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.

17 CUSTOMER DATA

17.1 The parties agree to the following provisions in connection with any Customer Data accessed, processed transmitted, 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.

17.2 Customer will be responsible for the accuracy and completeness of all Customer Data provided to Supplier by Customer. Customer shall retain exclusive ownership of rights, title, and interest in 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).

17.3 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.

17.4 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.

18 DATA SECURITY

18.1 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.

18.2 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. All Personal Data and Non-Public Data shall be subject to controlled access. Any stipulation of responsibilities shall be included in a Statement of Work and will identify specific roles and responsibilities.

18.3 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.

18.4 At no time shall any Customer Data or processes – that either belong to or are intended for the use of the State - be copied, disclosed, or retained by Supplier or any party related to Supplier for subsequent use in any transaction that does not include the State unless otherwise agreed to by the State.

18.5 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.

18.6 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.

18.7 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.

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

19 SECURITY ASSESSMENT

19.1 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.

19.2 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.

20 SECURITY INCIDENT OR DATA BREACH NOTIFICATION

20.1 Supplier shall inform Customer of any Security Incident or Data Breach.

20.2 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.

20.3 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).

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

20.5 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.

21 DATA BREACH NOTIFICATION AND RESPONSIBILITIES

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

21.1 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.

21.2 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.

21.3 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.

22 SUPPLIER REPRESENTATIONS AND WARRANTIES

Supplier represents and warrants the following:

22.1 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.

22.2 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.

22.3 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.

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

23 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.

24 TERMINATION, EXPIRATION AND SUSPENSION OF SERVICE

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

24.2 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.

24.3 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.

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

24.5 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.

25 GENERAL INFORMATION SECURITY REQUIREMENTS

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

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

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

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

26 HIPAA REQUIREMENTS

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

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

26.3 Business Associate Terms Definitions:

a. Unless otherwise defined in this BAA, all capitalized terms used in this BAA have the meanings ascribed in the HIPAA Regulations, provided; however, that "PHI" and "ePHI" shall mean Protected Health Information and Electronic Protected Health Information, respectively, as defined in 45 C.F.R. § 160.103, limited to the information Business Associate received from or created or received on behalf of the applicable State of Oklahoma agency as a Business Associate. "Administrative Safeguards" shall have the same meaning as the term "administrative safeguards in 45 C.F.R. § 164.304, with the exception that it shall apply to the management of the conduct of Business Associate's workforce, not the State of Oklahoma agency workforce, in relation to the protection of that information.

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

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

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

e. The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of

Privacy Practices, Protected Health Information, required by law, Secretary, Security Incident, Sub-Contractor, Unsecured PHI, and Use.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

26.6 Obligations of Covered Entity

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

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

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

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

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

26.7 <u>Term and Termination</u>:

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

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

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

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

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

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

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

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

26.8 Miscellaneous Provisions:

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

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

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

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

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

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

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

27 42 C.F.R. PART 2 RELATED PROVISIONS

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

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

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

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

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

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

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

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

27.9 Agrees to make available its internal practices, books, and records, including policies and procedures, relating to the use and disclosure of protected information received from the

State of Oklahoma agency or created or received by the Contractor on behalf of the State of Oklahoma agency, to the State of Oklahoma agency and to the Secretary of the Department of Health and Human Services for purpose of the Secretary determining the giving party's compliance with HIPAA;

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

28 DATA SECURITY

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

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

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

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

29 FEDERAL TAX INFORMATION REQUIREMENTS IRS PUBLICATION 1075

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

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

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

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

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

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

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

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

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

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

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

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

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

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

30 CRIMINAL/CIVIL SANCTIONS

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

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

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

30.4 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.

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

31 INSPECTION

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

32 SSA REQUIREMENTS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

33 CRIMINAL/CIVIL SANCTIONS

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

33.1 Civil Remedies

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

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

c. the costs of the action together with reasonable attorney fees as determined by the court.

d. An action to enforce any liability created under 5 U.S.C. § 552a may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where parties subject to this Agreement have materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under 5 U.S.C. § 552a, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action because of any injury sustained as the result of a disclosure of a record prior to September 27, 1975.

33.2 Criminal Penalties

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

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

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

34 CHILD SUPPORT FPLS REQUIREMENTS

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

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

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

35 FERPA REQUIREMENTS

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

36 CJIS REQUIREMENTS

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

36.2 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.

36.3 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."

36.4 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.

36.5 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.

36.6 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:

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

b. the general policies in §4;

c. the Policies in §5;

d. the appropriate forms in Appendices "D", "E", "F" & "H"; and

e. the Supplemental Guidance in Appendices "J".

36.7 This FBI Security Policy is located and may be downloaded at:

a. https://www.fbi.gov/services/cjis/cjissecurity-policy-resource-centerhttps://www.fbi.gov/services/cjis/cjissecurity-policy-resource-center.

b. 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.

37 NOTICES

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

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

<u>With a copy, which shall not constitute notice, to:</u>
OMES Deputy General Counsel
3115 North Lincoln Blvd
Oklahoma City, Oklahoma 73105

		State of Oklahoma Event # EV00000504 Ethics Commission - Political Finance Management System	Indicate Yes/No/WC With Configuration	Any documents provided in addition to the Bidder Response column below MUST be in searchable Word or .pdf file formats.
	Address and discuss each item below as it relates to your solution. Indicate if it is Out-of-the-Box, Not Offered, or is available With Configuration			
		Functionality	Y/N/WC	Comments/Answers
User Authentication and Authorization	1	The system will integrate with Azure Active Directory (AD) for single sign-on (SSO) authentication for users that are currently employed with the State of Oklahoma or hold a current AD account, enabling seamless access for state users using their existing credentials. All other users will be authenticated through a native solution.	Y	RFD's proposed solution will use Microsoft Entra Id (fka Azure AD) as an IDP, which will allow for seamless SSO for state users with their existing Entra IDs (fka Azure AD).
	2	A registration process will authenticate and verify individuals and organizations not included in state user authentication, ensuring access only for authorized parties.	Y	Users requiring only access to the public reporting/search functions will not require authorization. RFD will work with the ethics commission to identify and implement an appropriate registration flow for users not included in the state user pool.
	3	Role-based access control mechanisms will manage permissions for state users and registered entities, assigning roles based on responsibilities and permissions to control access to system features and data.	Y	RFD proposes to implement Role-Based Access Control (RBAC): RBAC is the most prevalent model in the industry. Access to resources is granted based on the roles assigned to users. Roles are defined based on job functions, and permissions are assigned to these roles. Users are then assigned to the appropriate roles, granting them the necessary permissions to perform their job functions.
	4	Public access to reporting functionalities will be available without login credentials, promoting data transparency initiatives.	Y	We understand the requirement and will implement this feature as requested.
User Activity Logs and Audit Trails	5	Comprehensive user activity logs and audit trails will record all user interactions, transactions, and system activities for accountability and compliance.	Y	RFD's proposed solution will leverage cloud provider native services and Elastic Observability to maintain audit trails for all desired and required system activities to maintain compliance.
	6	Activity logs will capture details such as login/logout events, data access, modifications, and administrative actions, ensuring transparency and facilitating regulatory compliance through chronological records.	Y	The application will track timestamps and the user who makes adds, deletes, or updates data in the system. A Login history will also be maintained and made available to authorized users.
Data Encryption in Transit and at Rest	7	The system will employ encryption protocols to secure data transmission between users' devices and the system (in transit) and when data is stored on servers or databases (at rest).	Y	Our proposed solution will implement strong TLS encryption protocols (min TLS 1.2) for all data in transit, and AES 256 encryption (or comparable) encryption for all data at rest.
	8	Encryption measures will ensure that sensitive information exchanged during the registration process or accessed by authenticated users remains confidential and protected from unauthorized access.	Y	Strong TLS and AES encryption will be implemented to secure all sensitive data exchanged during the registration process.
Cloud-Based Platform Delivery and Integration	9	The system will be deployed on a Software as a Service (SaaS) platform, hosted in the cloud, ensuring users always have access to the latest version without the need for manual updates or maintenance.	Y	The application will be deployed as a SaaS platform, updates and maintenance will be performed by RFD on a regular schedule. If down time is required for any updates RFD will work with the Oklahoma Ethics Commission to identify an acceptable maintenance window to minimize the impact on public and Ethics Commission users.
	10	Integration with Oklahoma's cloud environment, including Azure cloud and Adobe Experience Manager (AEM), will optimize performance, scalability, and reliability, aligning with the state's technical standards and cloud-first strategy.	Y	RFD proposes to implement this solution in Azure Cloud to align with the state's IT ecosystem. RFD understood the Q&A to indicate that integration with AEM would be done in a later phase. RFD will ensure that we do not preclude integration with AEM during development of the filing system.
	11	Compatibility with Azure cloud infrastructure will ensure efficient deployment, management, and ongoing support of the system, facilitating interoperability and alignment with the state's IT ecosystem.	Y	RFD proposes to implement this solution in Azure Cloud to align with the state's IT ecosystem.
	12	Integration with AEM will enhance content management and publishing capabilities, providing a user-friendly experience for accessing information and resources hosted on the state's website.	WC	RFD understood the Q&A to indicate that integration with AEM would be done in a later phase. RFD will ensure that we do not preclude integration with AEM during development of the filing system.
	13	The system will feature up-to-date data processing capabilities to handle incoming data streams and user interactions instantaneously, providing timely updates and responses to users.	Y	Incoming data will be processed real time and we will work with the Oklahoma Ethics commission to ensure that adequate capacity is built into the system to ensure acceptable response times even during heavy usage periods.

Data Processing and Analytics	14	Advanced analytics tools will enable users to perform interactive analysis of data, uncovering insights and trends to support decision-making and strategic planning.	Y	RFD proposes that Tableau be utilized for reporting and Analytics. Tableau is a powerful data visualization and business intelligence platform that enables users to perform advanced analytics and interactive analysis of data. These visualizations allow users to explore and analyze data, uncovering valuable insights and trends that support decision-making and strategic planning.
Reporting tools	15	The system will feature comprehensive reporting tools that allow users to generate various types of reports based on data stored within the system.	Y	With Tableau, users can connect to various data sources, such as databases, spreadsheets, and cloud applications, and create visually compelling dashboards, charts, and reports.
	16	Reporting tools will offer functionalities such as predefined report templates, customizable parameters, and ad-hoc report generation capabilities.	Y	Tableau's intuitive user interface and robust set of features make it easy for users to interact with data, perform complex calculations, and generate actionable insights, even without extensive technical or statistical expertise.
	17	Users will have the option to export reports in multiple formats such as PDF, Excel, CSV, and HTML, facilitating data analysis, sharing, and integration with external systems.	Y	Tableau provides users with the flexibility to export reports in various formats, including PDF, Excel, CSV, and HTML. This feature enables users to share their data analysis and insights with others, even if they do not have access to the Tableau platform.
Secure API Endpoints for Data Exchange	18	The system will be capable of providing secure API endpoints to facilitate seamless data exchange with external systems, applications, and services.	Y	RFD intends to utilize Azure API Management to secure API endpoints. Certificates will be obtained from a trusted authority and only TLS version 1.2 or above will be permitted. Each API will be configured to log incoming requests, including relevant information like client IP, request method, endpoint, and response status.
	19	API endpoints will be protected using industry-standard security protocols such as OAuth 2.0 authentication and HTTPS encryption to ensure data integrity and confidentiality.	Y	All API calls will be authenticated using token based security, if a request is made to an API with a missing or invalid token that request will not be permitted.
Automated Data Backups and Disaster Recovery	20	The system will implement automated data backup processes to regularly create and store copies of data in secure locations, ensuring data integrity and availability	Y	Our proposed solution will ensure all file and database data is backed up in real time or near real time to support point in time recovery, as well as nightly backups to an additional cloud region to support disaster recovery.
	21	Backup schedules will be configurable, allowing administrators to define frequency, retention policies, and backup destinations based on business requirements and compliance regulations.	Y	Confirmed all backups are configurable for retention and destination to meet any state requirements.
Electronic Signature Processing	22	The system will support electronic signature processing to facilitate the digital signing of documents and forms by authorized users.	Y	RFD proposes that DocuSign be used for ESIGN capabilities, there are many options on the market and we would be open to using a different provider if the state prefers.
	23	Electronic signature functionality will adhere to legal and regulatory standards such as the Electronic Signatures in Global and National Commerce (ESIGN) Act and the Uniform Electronic Transactions Act (UETA).	Y	DocuSign adheres to these requirements.
Document Management and Storage	24	The system will include robust document management and storage capabilities to organize, store, and retrieve documents and files securely.	Y	RFD proses that Elasticsearch be utilized for document management.
	25	Documents will be categorized, tagged, and indexed for easy search and retrieval, enabling users to locate relevant documents quickly.	Y	Elasticsearch is an industry leader in the document management space. Elasticsearch allows for easy ingesting and preprocessing of documents, creating an Elasticsearch index, indexing the preprocessed documents, categorizing and tagging them, providing a search interface for users, and tuning the relevance of search results to ensure efficient storage, retrieval, and user-friendly search experience.
	26	Allow users to pay fees online using Visa or Mastercard, AmX or Discover.	Y	We understand the requirement and will implement this feature as requested.
	27	Allow for online payments even when an administrative hearing is pending by changing the compliance fee status to "ALJ pending."	Y	We understand the requirement and will implement this feature as requested.
	28	Enhance user convenience and satisfaction by providing partial payment options. This would specifically be helpful with the late filing fees assessed and flexibility.	Y	We understand the requirement and will implement this feature as requested.
	29	Implement a system to receive notifications when users make online payments.	Y	We understand the requirement and will implement this feature as requested.
	30	When marking principals paid manually, provide an option to indicate the actual person (Lobbyist)who paid the principal to ensure clarity and accuracy in recording payment information.	Y	We understand the requirement and will implement this feature as requested.
	31	The system will include tools for managing financial transactions, such as accounts receivable, accounts payable, and general ledger functions.	Y	We understand the requirement and will implement this feature as requested.
	32	Users will be able to perform tasks such as recording transactions (contributions, expenditures, loans), generating invoices (Registration fees and late fees owed with total due to pay from), and reconciling accounts within the system's interface.	Y	We understand the requirement and will implement this feature as requested.

Financial Transaction Processing	33	Ability for Liaisons to print an invoice prior to paying registration. Liaisons need an invoice to request inter/intra agency transfer. capability to manually mark their registrations paid after pulling the Inter/Intra Agency Payments report.	Y	We understand the requirement and will implement this feature as requested.
	34	A system to only allow one payment of a lobbyist principal so that manually tracking and refunding of lobbyists for principal payments that were already made by another lobbyist is eliminated. Many principals have multiple lobbyists.	Y	We understand the requirement and will implement this feature as requested.
	35	A system to show the principal as paid across multiple lobbyists. The system accesses the Secretary of State data base ID numbers to accomplish this, but the lobbyist doesn't always select the same principal number if they have more than one in the SOS data base or the lobbyist cannot find their principal and they manually enter them.	Y	We understand the requirement and will implement this feature as requested.
	36	Ability to access all receipts to provide lobbyists needing a receipt for their registration.	Y	We understand the requirement and will implement this feature as requested.
Compliance Tracking and Reporting	37	The system will include features for tracking and reporting compliance with regulatory requirements, internal policies, and industry standards related to ethics, campaign finance, and lobbying activities.	Y	RFD has implemented similar features for the Texas Ethics Commission. Before a report can be filed all forms are evaluated for missing or invalid data. A series of more complex business rules are also run checking for things such as multiple Unitemized contributions from a single contributor adding up to a large enough contribution that everything must be itemized. The process known as the "error check" must be run before a report can be filed. It returns errors of High, Medium and Low. Per TEC guidance a report cannot be filed with a "High Error". A report can be filed with "Medium" and/or "Low" errors but the filer must acknowledge that they are filing with errors, if they do so the system tracks both the acknowledgement and the list of errors so that they can be reviewed by TEC and used in any enforcement action regarding the filer.
	38	Compliance tracking functionalities will enable users to monitor adherence to applicable laws and regulations, identify compliance gaps, and take corrective actions as necessary.	Y	Please see the description for item 37 above for an example of how we have implemented this type of feature before.
Stakeholder Communication Tools	39	The system will provide stakeholder communication tools to facilitate collaboration and communication among internal users, external stakeholders, and the public.	Y	There are a number of options for messaging features and notifications available. These can vary widely in terms of functionality and cost. RFD will work with the Oklahoma Ethics Commission to identify how best to meet these requirements within budget.
	40	Communication tools may include messaging features, discussion forums, and notification systems to keep stakeholders informed about relevant updates, events, and actions.	Y	There are a number of options for messaging features and notifications available. These can vary widely in terms of functionality and cost. RFD will work with the Oklahoma Ethics Commission to identify how best to meet these requirements within budget.
Training Modules and User Support Documentation	40	The system will offer comprehensive training modules and user support documentation to onboard new users, educate stakeholders, and provide ongoing support.	Y	RFD will produce user guides, tutorials and video trainings.
	41	Training modules will cover system functionalities, best practices, and compliance requirements, delivered through interactive tutorials, videos, and webinars.	Y	RFD will produce user guides, tutorials and video trainings.
Mobile Responsiveness and Cross-Platform Compatibility	42	The system will be designed with mobile responsiveness and cross-platform compatibility, ensuring optimal user experience and functionality across various devices and operating systems.	Y	RFD utilizes a mobile first approach to development. All pages are developed using fully responsive tools to ensure that the applications work on any modern screen or device regardless of size.
Feedback Collection and Management System	43	The system will include a feedback collection and management system to gather input from users, stakeholders, and the public.	Y	RFD proposes a contact us feature to satisfy the requirement to address user inquiries.
	44	Feedback mechanisms may include surveys, suggestion boxes, and feedback forms integrated within the system.	Y	RFD proposes a contact us feature to satisfy the requirement to address user feedback and suggestions. RFD will work with the state to identify a third party solution for surveys that will meet survey requirements within budget.
	45	System monitoring and performance analytics tools will be implemented to track the health, availability, and performance of the system.	Y	RFD will use Elastic Observability for system monitoring and performance monitoring. Elastic Observability is a comprehensive system monitoring and performance analytics tool designed to track the health, availability, and performance of IT systems. By leveraging artificial intelligence and machine learning, Elastic Observability automatically discovers and maps all components of the system, including servers, applications, and services, providing real-time insights into their performance and interdependencies. Users can proactively monitor system health, identify performance bottlenecks, and resolve issues before they impact end-users. The platform's advanced analytics and root cause analysis capabilities enable users to optimize system performance, ensure high availability, and improve overall user experience.

System Monitoring and Performance Analytics	46	These tools will monitor key metrics such as uptime, response times, and resource utilization to proactively identify and resolve issues.	Y	Elastic Observability monitors key metrics such as uptime, response times, and resource utilization to proactively identify and resolve issues. By continuously tracking these critical indicators, Elastic Observability enables users to detect performance anomalies and potential problems in real-time. The platform's AI-powered analytics engine analyzes the collected data, providing actionable insights and intelligent alerts that help users quickly pinpoint the root cause of issues and take corrective action.
Data Migration Tools and Services	47	Data migration tools and services will be provided to facilitate the transfer of data from legacy systems or external sources to the new system.	Y	RFD understands and will comply.
	48	These tools will support various data migration scenarios, including schema mapping, data cleansing, and validation.	Y	RFD will work with the Oklahoma Ethics Commission to identify data cleansing rules. A data mapping document will be provided that shows where data is coming from and where it is being migrated to in order to ensure completeness and accuracy. While validation checks will be executed during migration RFD believes that testing the application on migrated data as soon as possible is key to ensuring data quality. We will include this as part of our validation efforts.
SLA Management and Tracking	49	Service Level Agreement (SLA) management and tracking functionalities will be incorporated to define, monitor, and enforce service level commitments.	Y	Elastic Observability can establish SLAs based on key performance indicators (KPIs) such as response times, availability, and error rates.
	50	SLAs will specify performance metrics, response times, availability targets, and support obligations to ensure that service levels meet agreed-upon standards.	Y	Elastic Observability continuously monitors the system's performance against these SLAs, providing real-time visibility into compliance status and alerting users when SLAs are at risk of being breached.
Campaign Finance Management	51	Comprehensive tools for tracking, reporting, and analyzing campaign contributions and expenditures will be provided.	Y	We understand the requirement and will implement this feature as requested.
	52	Features include automation of data entry, real-time compliance monitoring, and auditing capabilities.	Y	We understand the requirement and will implement this feature as requested.
Advanced Search and Reporting	53	The system will enable complex data queries and custom report generation for in-depth analysis.	Y	Tableau enables users to perform complex data queries and generate custom reports for in-depth analysis.
	54	Features include filter options for specific criteria, export capabilities, and pre-configured report templates.	Y	With Tableau's intuitive drag-and-drop interface and powerful data manipulation capabilities, users can easily explore and analyze large datasets, regardless of their technical expertise.
Customizable Dashboards for Different User Roles	55	Personalized dashboards will be provided for different user roles, displaying relevant information and tasks.	Y	Tableau enables the creation of personalized dashboards tailored to different user roles, ensuring that each user has access to relevant information and tasks.
	56	Dashboards will prioritize relevant data and actions based on the user's role.	Y	With tableau we can create role-specific views that display the most critical data points, key performance indicators, and actionable insights for each user group. This targeted approach to data visualization helps users focus on the information that matters most to them.
Legislative and Regulatory Compliance	57	The system will be built to adapt to changes in laws and regulations, maintaining compliance without significant system overhauls.	Y	RFD strives to develop applications that are configurable and are easy to maintain. Major changes in stature will no doubt require application code changes. Our development methodologies allows us to minimize those changes to the extent that we can.
	58	Mechanisms for updating the platform in response to new legislative requirements will be included.	Y	RFD strives to develop applications that are configurable and are easy to maintain. Major changes in stature will no doubt require application code changes. Our development methodologies allows us to minimize those changes to the extent that we can.
Ease of Integration	59	The system will seamlessly integrate with software commonly used by PACs and other political finance groups.	Y	RFD will develop an API for external groups to interface with the system.
	60	Integration capabilities will promote efficiency in data management and reporting.	Y	RFD will develop an API for external groups to interface with the system.
	61	Integration points for NAVEX Global and other similar Ethics reporting software used by PACs preferred.	Y	RFD will develop an API for external groups to interface with the system.
Non-SOS principal listing	62	Non-SOS Principal listings must undergo an SOS search initially.	Y	We understand the requirement and will implement this feature as requested.
	63	If not found in SOS, system can assign a system number upon entry.	Y	We understand the requirement and will implement this feature as requested.
	64	Subsequent entries will search SOS first, then possibly match to a system, automatically marking payments.	Y	We understand the requirement and will implement this feature as requested.
Procedure for deceased PFD filer	65	Establish a procedure for handling deceased PFD filers, with the use of the Terminate option and documenting the last day of service in the Administrator Notes.	Y	We understand the requirement and will implement this feature as requested.
Name of filer on IE/EC/SQC Reports	66	Relocate the filers name from the top to the bottom of the IE/EC/SQC reports.	Y	We understand the requirement and will implement this feature as requested.
Ending balance check	67	Enable the system to generate a list of ending balances as a double check on closing.	Y	We understand the requirement and will implement this feature as requested.
In-Kind Expenditure	68	The system should present In-Kinds expenses line items in a grid regardless of their value being under $200, like candidate reimbursement.	Y	We understand the requirement and will implement this feature as requested.

Transfer In and Transfer Out of Funds	69	The system should utilize the same language during transfer in and out of Funds to associated Committee not registered. The language should be on both Prior Committee Not Registered (because they terminated before making the transfer) and the interior language right now refers to PACs it should follow the Candidate Transfer in and out from prior committee language.	Y	We understand the requirement and will implement this feature as requested.
Batch, email election specific	70	Provide the option to select specific election cycles for batch email instead of sending to all candidates. Provide the option to select specific election cycles for batch email instead of sending to all candidates.	Y	We understand the requirement and will implement this feature as requested.
Lobbyist principal number assignments	71	Get rid of SOS lookup and implement a system to assign unique numbers to lobbyist principals, Search list when registering to avoid double payments.	Y	We understand the requirement and will implement this feature as requested.
Candidates' district/ Office – pending registration	72	Include a column displaying the Candidate's District/Office in pending registrations.	Y	We understand the requirement and will implement this feature as requested.
Multiple choices	73	Modify the system to require dual-registered lobbyists to choose both legislature/Governor/Staff and at least one executive agency. Include a dropdown option to choose previous recipients if the recipient is a state officer or employee.	Y	We understand the requirement and will implement this feature as requested.
Acronym Display	74	Display the "Acronym" from the Statement of Organization in the Committee section of the system if available.	Y	We understand the requirement and will implement this feature as requested.
User-friendliness Interface	75	Design intuitive user interfaces with clear navigation, consistent layouts, and contextual help features to enhance usability and user satisfaction.	Y	We understand the requirement and will implement this feature as requested.
	76	Add the system's ID number to dropdown lists for PAC or Party for Candidates. (Ex. BONDSMAN POLITICAL ACTION COMMITTEE (ID: 1234)	Y	We understand the requirement and will implement this feature as requested.
	77	Allow users to search through time for lobbyist principals historically, showing all instances regardless of active or terminated status. Add a column to display the years during which a lobbyist principal was represented by a particular lobbyist in administrative reports.	Y	We understand the requirement and will implement this feature as requested.
	78	Enable REFUND search and a keyword search in public site for expenditures and contributions pages by description (keyword search)	Y	We understand the requirement and will implement this feature as requested.
	79	Include "revert to pending registration" and/or "delete" buttons in the conditional acceptances grid to enable COs to manage pending registrations effectively and rectify accidental status changes.	Y	We understand the requirement and will implement this feature as requested.
	80	Provide an option to opt-in to receiving text notifications for report due reminders upon committee registration and enable users to input their phone numbers for receiving text messages when they opt in.	Y	We understand the requirement and will implement this feature as requested.
	81	Conduct usability testing and gather feedback from users to iteratively improve the user experience and address usability issues.	Y	RFD will work with the Oklahoma Ethics Commission to identify users who can assist with testing for user experience and usability. We will address any agreed upon changes in a timely manner.
	82	Ensure that the system's user interface complies with the accessibility standards outlined in the Oklahoma Electronic and Information Technology Accessibility (EITA) Act to provide equal access to users with disabilities.	Y	RFD takes accessibility very seriously, we use a variety of tools to ensure that code meets WCAG standards including screen readers and scanning tools such as Axe.
Performance efficiency	83	Optimize system performance to ensure fast response times, minimal latency, and efficient resource utilization under varying workloads.	Y	RFD utilizes Elastic Observability during all phases of development, from initial development, system test, user acceptance test, and performance testing. We also utilize Elastic Observability once the application is live to provide users with actionable insights and recommendations for optimizing resource allocation, reducing bottlenecks, and improving overall system efficiency.
	84	Implement performance monitoring and tuning mechanisms to identify performance bottlenecks and optimize system throughput and responsiveness.	Y	RFD utilizes Elastic Observability during all phases of development, from initial development, system test, user acceptance test, and performance testing. We also utilize Elastic Observability once the application is live to provide users with actionable insights and recommendations for optimizing resource allocation, reducing bottlenecks, and improving overall system efficiency.
	85	Design the system architecture to scale horizontally and vertically to accommodate growing user bases and increasing data volumes.	Y	RFD's proposed architecture will utilize cloud native technologies for multi-availability zone autoscaling, database replicas (ready for promotion) as well as storage autoscaling where possible to ensure the solution is available and performant for any demand that the users may generate.

Scalability	86	Utilize cloud-based infrastructure and elastic scaling capabilities to dynamically allocate resources based on demand fluctuations and workload patterns.	Y	RFD's proposed architecture will utilize cloud native technologies for multi-availability zone autoscaling, database replicas (ready for promotion) as well as storage autoscaling where possible to ensure the solution is available and performant for any demand that the users may generate.
Performance efficiency	87	Optimize system performance to ensure fast response times, minimal latency, and efficient resource utilization under varying workloads.	Y	RFD utilizes Elastic Observability during all phases of development, from initial development, system test, user acceptance test, and performance testing. We also utilize Elastic Observability once the application is live to provide users with actionable insights and recommendations for optimizing resource allocation, reducing bottlenecks, and improving overall system efficiency.
	88	Implement performance monitoring and tuning mechanisms to identify performance bottlenecks and optimize system throughput and responsiveness.	Y	RFD utilizes Elastic Observability during all phases of development, from initial development, system test, user acceptance test, and performance testing. We also utilize Elastic Observability once the application is live to provide users with actionable insights and recommendations for optimizing resource allocation, reducing bottlenecks, and improving overall system efficiency.
Reliability	89	Implement fault-tolerant and resilient system components with redundancy, failover mechanisms, and automated recovery processes to ensure high system availability.	Y	RFD's proposal takes advantage of cloud native autoscaling features with health checks and load monitoring to ensure resources are always available to meet demand, and unhealthy resources are replaced automatically without impact to availability. Azure database storage and Azure blob storage are highly durable storage solutions (Azure blob offers 11 9's of availability). Azure database backups offer point in time restore capabilities as well.
	90	Conduct regular reliability testing and simulations to validate system resilience and identify potential points of failure for proactive mitigation.	Y	RFD's proposed solution uses the native cloud services to support deployment and update processes as part of standard operating procedures, which is an excellent test bed for these features. For any services that are not regularly exercised in this way, RFD will test at an appropriate frequency to ensure any unplanned incidents recover as expected.
Maintainability	91	Adopt modular and well-documented coding practices to facilitate code maintainability, readability, and extensibility.	Y	RFD developers are some of the best in the world, we adhere to industry standards in our coding Practice. We use tools such as SonarQube to automated code quality analysis to check for things such as duplicate code, excess cyclomatic complexity, and potential security risks .
	92	Establish version control, code review, and documentation standards to streamline collaboration among development teams and promote continuous improvement.	Y	All source code is stored in version control tools. RFD leverages industry best practices for CI/CD. All code is built and scanned for quality on every check in. We use branching strategies to ensure code is separate until it has been fully tested and is ready to be merged with the production branch. In addition before code can be merged to a main branch it must undergo peer code review to ensure quality.
Regulatory compliance	93	Ensure compliance with relevant regulations, industry standards, and legal requirements such as HIPAA, and PCI-DSS.	Y	RFD strives to build secure systems that keep confidential data confidential. The application will adhere to PCD-DSS standards along with industry standard security requirements. HIPPA compliance is specific to health insurance information, if the application contains HIPPA data we will ensure that we are in compliance with those regulations. Even when an application does not contain HIPPA data we strive to be in compliance with the standards it sets out.
	94	Implement data governance policies, access controls, and audit trails to demonstrate regulatory compliance and mitigate legal risks.	Y	RFD has internal governance policies and understands that the state of Oklahoma has them as well. We will work with the Ethics Commission to identify an agreed upon set of policies and can leverage Azure native tools such as Azure Information Protection, Azure Policy, and Azure Compliance Manager to assist with these requirements.
	95	Ensure compliance with the Oklahoma Ethics Commission's reporting requirements, including but not limited to transparency in lobbying activities, campaign finance disclosures, and ethics reporting for public officials and employees, as mandated by Title 74 of the Oklahoma Statutes, Section 62.1 et seq.	Y	RFD has implemented similar features for the Texas Ethics Commission. Before a report can be filed all forms are evaluated for missing or invalid data. A series of more complex business rules are also run checking for things such as multiple Unitemized contributions from a single contributor adding up to a large enough contribution that everything must be itemized. The process known as the "error check" must be run before a report can be filed. It returns errors of High, Medium and Low. Per TEC guidance a report cannot be filed with a "High Error". A report can be filed with "Medium" and/or "Low" errors but the filer must acknowledge that they are filing with errors, if they do so the system tracks both the acknowledgement and the list of errors so that they can be reviewed by TEC and used in any enforcement action regarding the filer.
	96	Enforce robust security measures, including encryption, authentication, authorization, and intrusion detection, to protect sensitive data and prevent unauthorized access.	Y	RFD's proposed solution will meet or exceed all best practice, Industry frameworks and regulatory requirements for this through an array of tools including cloud native and third party services. We start with a principal of least privilege, strong encryption (TLS 1.2 & AES256) and proven authentication and authorization services centered around Azure Entra ID (fka Azure AD). Microsoft Defender, Sentinel and Elastic Observability provide XDR, next gen AV and malware, intelligent threat detection and SIEM & SOAR capabilities. Elastic Observability CSPM and Azure native services will provide secure posture analysis and aid in proactively closing any vulnerable surface areas.
	97	Conduct regular security assessments, vulnerability scans, and penetration testing to proactively identify and address security vulnerabilities.	Y	All source code is scanned each time it is checked in for potential security issues using SonarQube. Additionally RFD utilized Snyk to scan third party libraries for vulnerabilities and patches critical and high vulnerabilities as soon as possible. Per the RFP requirements we will conduct annual penetration testing on the production system.

Security	98	Enforce robust security measures, including encryption, authentication, authorization, and intrusion detection, to protect sensitive data and prevent unauthorized access in accordance with the Oklahoma State Government IT Security Policies.	Y	RFD's proposed solution will meet or exceed all best practice, industry frameworks and regulatory requirements for this through an array of tools including cloud native and third party services. We start with a principal of least privilege, strong encryption (TLS 1.2 & AES256) and proven authentication and authorization services centered around Azure Entra ID (fka Azure AD). Microsoft Defender, Sentinel and Elastic Observability provide XDR, next gen AV and malware, intelligent threat detection and SIEM & SOAR capabilities. Elastic Observability CSPM and Azure native services will provide secure posture analysis and aid in proactively closing any vulnerable surface areas.
Technical support and training	99	Provide comprehensive technical support services including helpdesk support, knowledge base resources, and user training programs to assist users with system usage and troubleshooting, meeting the support requirements outlined by the Oklahoma State Ethics Commission.+	Y	RFD will provide help desk support to the administrative users of the system, we will also be available to assist with answering any questions posed to Oklahoma Ethics Commission by filers or the public that the Oklahoma Ethics Commission cannot answer on their own regarding the system.
Service Level Agreements (SLAs)	100	Define SLAs with clear objectives, metrics, and performance targets for system availability, response times, and support responsiveness in alignment with the Oklahoma State Government IT Service Level Agreement Guidelines.	Y	Elastic Observability can establish SLAs based on key performance indicators (KPIs) such as response times, availability, and error rates. Elastic Observability continuously monitors the system's performance against these SLAs, providing real-time visibility into compliance status and alerting users when SLAs are at risk of being breached.
Accessibility compliance	101	Ensure accessibility for users with disabilities by adhering to accessibility standards such as WCAG and Section 508, as mandated by the Oklahoma Electronic and Information Technology Accessibility (EITA) Act.	Y	RFD takes accessibility very seriously, we use a variety of tools to ensure that code meets WCAG standards including screen readers and scanning tools such as Axe.
System and data migration smoothness	102	Ensure seamless migration of existing data and systems to the new platform, minimizing downtime and data loss during the transition process.	Y	RFD intends to migrate all possible data and will generate validation routines to run during and after the conversion to ensure all data that should be migrated is. RFD will work with the Oklahoma Ethics Commission to identify a migration window sufficient to complete and test the migration that provides for the least amount of down time.
Interoperability with existing state systems	103	Facilitate seamless integration and data exchange with other state systems, ensuring compatibility and interoperability to support cross-functional processes and information sharing.	Y	RFD will work with the Oklahoma Ethics Commission to document the required interfaces with existing systems and develop file exchanges processes or API's as needed to ensure interoperability.
Adaptability to future technological advancements or legislative changes	104	Design the system architecture and functionalities to be adaptable and flexible, allowing for seamless integration of future technological advancements and legislative changes without requiring significant system redesign or redevelopment.	Y	RFD strives to develop applications that are configurable and are easy to maintain. Major changes in stature will no doubt require application code changes. Our development methodologies allows us to minimize those changes to the extent that we can.
Ease of system customization without extensive coding	105	Provide user-friendly tools and interfaces for system customization, allowing administrators to tailor system configurations, workflows, and user interfaces to meet specific requirements without the need for extensive coding or technical expertise.	Y	RFD strives to develop applications that are configurable and are easy to maintain. We will work with the Oklahoma Ethics Commission to identify items that can be configuration only and focus on those. Given the short implementation timeframe choices will have to be made about what can be configuration only and what will require code changes.
Clear documentation for both users and administrators	106	Provide comprehensive documentation for users and administrators, including user guides, technical manuals, and troubleshooting resources, to facilitate system usage, configuration, and maintenance tasks.	Y	RFD will produce user guides, tutorials and video trainings that will be accessible from the main application. RFD will produce technical documentation including a Software Design Document as well as cloud and application architecture documentation.
SLA specifics including uptime guarantees and compensation mechanisms	107	Define clear Service Level Agreement (SLA) specifics, including uptime guarantees, performance metrics, and compensation mechanisms for any service disruptions or breaches of agreed-upon service levels.	Y	RFD will deliver a high availability system that will exceed 99.9 % up time excluding planned maintenance or other planned outages. If an instance occurs where uptime falls below 99.9% and the cloud provider is at fault RFD will return any credits or compensation to the state of Oklahoma. For example, if the Azure Compute SLA of 99.9% uptime is not met, customers may be eligible for a 10% service credit if the uptime falls between 99.0% and 99.9%, a 20% credit if it falls between 98.0% and 99.0%, and so on.
Robust monitoring tools for system performance and health	108	Deploy comprehensive monitoring tools to track system performance, health, and resource utilization in real-time, enabling proactive identification of performance issues or bottlenecks for timely resolution.	Y	Elastic Observability provides comprehensive monitoring tools to track system performance, health, and resource utilization in real-time, enabling proactive identification of performance issues or bottlenecks for timely resolution.

Data portability to allow easy data extraction	109	The proposed solution must include robust data portability capabilities to ensure easy and secure data extraction and migration. This should encompass the ability to export data in a variety of standard file formats such as CSV, JSON, XML, or via APIs that enable seamless integration with other systems. The solution should facilitate the extraction of complete datasets or selective data based on specific criteria, ensuring compatibility with different platforms and software used by state agencies or third-party entities. Vendors should detail their approach to data portability, including any tools or services provided that support data extraction, migration, and the long-term usability of data outside the proprietary system. This specification should also cover methods for data backup, restoration, and the transfer of data without data loss or corruption, adhering to the latest security and compliance standards.	Y	There are numerous options for exporting of data in the required formats. Once we understand the full requirements we will be able identify the best solution for exporting data in these formats for this project. RFD will provide interfaces and integrations as required. In some cases a key component of the system we propose to develop is our proprietary flat file architecture could be used. It is an essential part of the Texas Ethics Commission's Electronic Filing System, allowing for exports of files in various formats. Tableau also allows for exporting to different formats also allows users to integrate Tableau-generated reports with external systems, such as reporting tools, databases, or other business applications, enhancing the platform's interoperability and utility.

State of Oklahoma Event
#EV00000504
Ethics Commission - Political
Finance Management System

Any documents provided in addition to the Bidder Response column below MUST be in searchable Word or .pdf file formats.

Discuss each item below as it relates to your proposed solution.

	Response Table	Bidder Response
	Oklahoma cloud environment compatibility	
1	Ensure compatibility with Oklahoma's preferred cloud infrastructure provider, Azure, adhering to Azure's recommended architectural patterns and best practices for cloud-native application development, if applicable.	RFD understands compatibility with existing Oklahoma infrastructure along with integrations are paramount to the success of the project, and will have no problem meeting or exceeding expectations. We are proposing implementation in Azure, however we are confident in delivering in any Cloud provider should formal discovery and design suggest another provider may be better for the overall success of the project. RFD is well versed in Cloud native design and considers cloud service provider well architected frameworks a guiding principle and adherence a key success metric
2	Utilize Azure services such as Azure Active Directory (AD) for user authentication for state users only.	RFD understands and has no concerns with supporting SSO for state users Azure AD/Entra ID identities to the new solution.
	AEM website framework integration	
3	Integrate seamlessly with Adobe Experience Manager (AEM) using industry-standard protocols such as RESTful APIs or Adobe's provided SDKs to enable content management and publishing capabilities within the system, where business needs dictate.	RFD understood the Q&A to indicate that integration with AEM would be done in a later phase. RFD will ensure that we do not preclude integration with AEM during development of the filing system.
4	Adhere to AEM's recommended practices for integration, including proper handling of content structure, metadata, and asset management to ensure consistency and accuracy in web content delivery.	RFD understood the Q&A to indicate that integration with AEM would be done in a later phase. RFD will ensure that we do not preclude integration with AEM during development of the filing system.
	Cloud-based hosting	
5	Implement cloud-based hosting to leverage the scalability, reliability, and accessibility benefits of a Software as a Service (SaaS) platform, ensuring users always have access to the latest version of the system without manual updates or maintenance.	The application will be deployed as a SaaS platform, updates and maintenance will be performed by RFD on a regular schedule. If down time is required for any updates RFD will work with the Oklahoma Ethics Commission to identify an acceptable maintenance window to minimize the impact on public and Ethics Commission users.
	Data encryption and security protocols	
6	Implement data encryption and security protocols that meet or exceed the encryption standards and security guidelines mandated by the state of Oklahoma for protecting sensitive information.	RFD will adhere to the mandated security guidelines. For example all data will be encrypted at rest and transit, outdated protocols such as TLS 1.0/1.1 will not be enabled in the system.
	Role-based access control	
7	Implement role-based access control (RBAC) mechanisms to manage user permissions and access rights based on their roles and responsibilities, ensuring that each user has appropriate access to system features and data.	RFD proposes to implement Role-Based Access Control (RBAC): RBAC is the most prevalent model in the industry. Access to resources is granted based on the roles assigned to users. Roles are defined based on job functions, and permissions are assigned to these roles. Users are then assigned to the appropriate roles, granting them the necessary permissions to perform their job functions.
	Two-factor authentication	
8	Two-factor authentication Two-factor authentication(2FA) involves adding extra security to your systems or accounts beyond just a password. You will need to provide a second form of identification. · The system should incorporate two-factor authentication (2FA) mechanisms to enhance user authentication security, aligning with state requirements for multi-factor authentication.	The RFD proposed solution will take advantage of the CSP provided 2FA features, for example Microsoft Entra ID (fka Azure AD) offers 2FA options such as email one time passwords and SMS based auth. RFD will work with the state to define the optimal configurations during formal discovery and design.
	APIs for third-party integration	

9	Prepared to provide secure APIs for seamless integration with third-party systems, applications, and services, enabling data exchange and interoperability to enhance system functionality and meet specific business requirements.	RFD intends to utilize Azure API Management to secure API endpoints. Certificates will be obtained from a trusted authority and only TLS version 1.2 or above will be permitted. Each API will be configured to log incoming requests, including relevant information like client IP, request method, endpoint, and response status. All API calls will be authenticated using token based security, if a request is made to an API with a missing or invalid token that request will not be permitted. APIs will be protected by one or more of the following depending on API use case: web application firewall, API key, throttling, rate limiting to further ensure security and protect from malicious activity.
	Responsive web design	
10	Design the system with responsive web design principles to ensure optimal user experience and functionality across various devices and screen sizes, including smartphones, tablets, and desktops, enhancing accessibility and usability for all users.	RFD utilizes a mobile first approach to development. All pages are developed using fully responsive tools to ensure that the applications work on any modern screen or device regardless of size.
	Data migration support	
11	Include data migration support features to facilitate the transition from legacy systems to the new system, complying with state guidelines for data migration and data integrity.	Analyzing and converting existing data will be an iterative process consisting of 4 phases: 1 - Discovery and Design - During this phase RFD will produce data mapping documents and will work with the Oklahoma Ethics Commission to establish data cleansing rules. 2 - Development and Unit Test - During 2 RFD will develop and validate the migration routines. 3 - System Integration Test - Phase 3 will overlap with phase 2 once a critical mass of data is being migrated. I our experience it is imperative to begin testing converted and test data created by the application as early as possible. This allows us to easily spot any discrepancies between the two sources of data and correct them early on. 4 - User Acceptance Test - RFD recommends that the Oklahoma Ethics Commission utilize the application to validate migrated data whenever possible. We will also produce metrics from the migration to help the Commission validate that all data that should be migrated was migrated.
	High availability and disaster recovery planning	
12	Implement high availability and disaster recovery planning to ensure system uptime, reliability, and resilience against unforeseen disruptions or disasters, minimizing downtime and data loss to maintain business continuity.	RFDs proposed solution design includes high availability utilizing native cloud services to deploy a network topology that spans multiple availability zones (~data centers), autoscaling groups to distribute compute resources across the multiple availability zones, and health checks to ensure only healthy resources receive traffic and autoscaling can balance and replace resources as needed. All resources will be resilient across availability zones such that the solution can withstand the complete destruction of one or more availability zones with minimal to zero service interruption. Our proposal includes a read replica for database servers, to offload read only traffic and to additionally act as a failover in the event of a failure of the primary node. The solution will also leverage Azure blob storage as the primary file store, a service which delivers at least 11 9's of availability ensuring data durability.
	User management system	
13	Implement a user management system that meets the state's requirements for user authentication, authorization, and account management, ensuring compliance with Oklahoma's standards for user access control.	RFD proposes to implement Role-Based Access Control (RBAC): RBAC is the most prevalent model in the industry. Access to resources is granted based on the roles assigned to users. Roles are defined based on job functions, and permissions are assigned to these roles. Users are then assigned to the appropriate roles, granting them the necessary permissions to perform their job functions. Authentication will be through Entra Id (fka Azure AD), and will support SSO for state users and their existing Entra ID/Azure AD Ids. MFA will be implemented where needed and users with access to application and cloud resources will function under a least privilege model.
	Advanced reporting and analytics tools	

14	Implement a suite of reporting and analytics tools that offer customizable dashboards, ad-hoc report generation, and advanced data visualization capabilities for administrator only. The dashboard should be uniform for the public site.	RFD proposes that Tableau be used for dashboards, ad-hoc report generation, and advanced data visualization capabilities. If Oklahoma has existing capacity for Tableau or another reporting and analytics tool such as Power BI, we would be open to utilizing that capacity to reduce costs for the state.
15	Ensure compatibility with common data formats and integration with popular analytics platforms for seamless data analysis and decision support.	Tableau can accept data from a number of formats including but not limited to Flat Files, Relational databases and big data solutions. In addition to supporting various data formats, Tableau also allows for integration with many popular analytics platforms.
	Electronic signature capabilities	
16	Integrate electronic signature functionality compliant with industry standards such as ESIGN and UETA.	RFD proposes that DocuSign be used for ESIGN capabilities, there are many options on the market and we would be open to using a different provider if the state prefers.
17	Provide secure authentication methods and audit trails for electronic signatures to ensure legal validity and authenticity.	DocuSign provides these features.
	Performance optimization	
19	Employ performance tuning techniques such as query optimization, caching mechanisms, and load balancing to enhance system responsiveness and throughput.	RFD uses Elastic Observability APM to identify queries that can be optimized, potential areas for caching optimization and to understand where on the system the heaviest and lightest load is being places. Utilizing the information from Elastic our developers and cloud engineers are able to tune the application and cloud infrastructure to optimize performance.
20	Conduct regular performance testing and monitoring to identify bottlenecks and optimize resource utilization for optimal user experience.	Elastic Observability monitors key metrics such as uptime, response times, and resource utilization to proactively identify and resolve issues. By continuously tracking these critical indicators, Elastic enables users to detect performance anomalies and potential problems in real-time. The platform's AI-powered analytics engine analyzes the collected data, providing actionable insights and intelligent alerts that help users quickly pinpoint the root cause of issues and take corrective action.
	Scalability provisions	
21	Design the system architecture with scalability in mind, utilizing scalable cloud services and elastic computing resources.	RFD's proposed design includes native cloud services for autoscaling of dedicated compute resources where needed allowing the solution to provision the resources needed to meet peek and valley demands with no administrative overhead nor wasted resources. Serverless compute resources will be implemented where it makes sense, which provides a major advantage in scalability agility and even better optimization of provisioned resources driving down costs. Storage is autoscaling and helps minimize administrative overhead.
22	Implement auto-scaling capabilities to dynamically adjust resource allocation based on demand fluctuations to maintain performance and availability.	RFD's proposed design includes native cloud services for autoscaling of dedicated compute resources where needed allowing the solution to provision the resources needed to meet peek and valley demands with no administrative overhead nor wasted resources. Serverless compute resources will be implemented where it makes sense, which provides a major advantage in scalability agility and even better optimization of provisioned resources driving down costs. Storage is autoscaling and helps minimize administrative overhead.
	Reliability standards	
23	Adhere to reliability best practices such as fault tolerance, redundancy, and failover mechanisms to ensure high system availability and resilience against failures.	In short, RFD's proposed solution can in its entirety survive an entire availability zone/data center failure with minimal to zero service disruption. To achieve this RFD will implement compute autoscaling health checks that ensure the optimal number of healthy resources are provisioned based on demand, and any unhealthy resources are promptly replaced without service interruption. Application data will never be stored locally on compute instances. All other networking resources will be provisioned redundantly across multiple availability zones ensuring application availability even in the event of a major data center service disruption. Azure blob storage provides a minimum of 11 9's of availability ensuring excellent data durability. Database compute will also include a read replica node in a different availability zone from the primary node, and will act to lower read load on the primary node and may also be promoted to primary node, should the primary node become unavailable for any reason. Database storage is spread across multiple availability zones and can survive a full az/data center disruption. All data is backed up to a separate region (geographically distanced to de-risk a single natural or other disaster from disrupting two regions) and can be used in disaster recovery.

24	Implement proactive monitoring and alerting systems to detect and address issues before they impact users.	RFD is an Elastic partner and will deploy the Elastic Observability platform that provides deep application and infrastructure insights through log & metric aggregation, APM (application performance management) integration, and CSPM integration (amongst others). Notifications and auto-remediation support ensure our operations team is aware, often before users, that there is an imminent or active issue. Through the APM integration, we get deep insights into the application behavior through infrastructure, application, application server, and runtime metrics, logs and stack calls all weaved together for simplicity. This drives down mean time to identification and remediation of issues.
	System maintainability	
25	Follow modular and well-documented coding practices to facilitate code maintainability and extensibility.	RFD developers are some of the best in the world, we adhere to industry standards in our coding Practice. We use tools such as SonarQube to automated code quality analysis to check for things such as duplicate code, excess cyclomatic complexity, and potential security risks .
26	Establish version control and release management processes to streamline updates, patches, and bug fixes while minimizing disruptions to operations.	All source code is stored in version control tools. RFD leverages industry best practices for CI/CD. All code is built and scanned for quality on every check in. We use branching strategies to ensure code is separate until it has been fully tested and is ready to be merged with the production branch. In addition before code can be merged to a main branch it must undergo peer code review to ensure quality.
	Regulatory compliance adherence	
27	Conduct thorough compliance assessments to identify applicable regulations and standards, including GDPR, HIPAA, and SOX.	RFD strives to build secure systems that keep confidential data confidential. The application will adhere to PCD-DSS standards along with industry standard security requirements. HIPPA compliance is specific to health insurance information, if the application contains HIPPA data we will ensure that we are in compliance with those regulations. Even when an application does not contain HIPPA data we strive to be in compliance with the standards it sets out.
28	Implement data encryption, access controls, and audit trails to meet regulatory requirements for data security and privacy.	RFD's proposed solution will deliver security in layers that will ensure the data is always safe when in transit or when at rest. We will deploy strong TLS encryption (min v1.2), AES 256 encryption of data at rest. RFD s proposed solution will leverage CSP provided security and audit tools, as well we intend to layer on Microsoft Defender and Elastic Observability platform to further aid providing audit trails, visibility and benchmarks to assess and remedy the cloud infrastructure and application security posture with respect to industry frameworks like NIST & CIS, CSP best practices and all regulatory requirements with confidence. RFD has no concerns that our solution will meet or exceed any and all expected security requirements.
	Security measures against data breaches	
29	Implement multi-layered security measures including encryption at rest and in transit, intrusion detection systems, and regular security audits and penetration testing.	RFD's proposed solution will deliver security in layers that will ensure the data is always safe when in transit or when at rest. We will deploy strong TLS encryption (min v1.2), AES 256 encryption of data at rest. Publicly exposed endpoints (CDN, API, Load balancers) will be protected by web application firewalls. APIs will be secured with access tokens. Endpoints will use Defender endpoint protection to provide EDR, next gen AV and malware protection, intelligent threat detection, IT hygiene and more. Cloud infrastructure will be monitored and assessed in near real time via cloud security posture management (CSPM) instrumentation. Our CSPM tool with give us real time visibility into desired state vs current state to assist in keeping posture in line with industry frameworks (CIS, NIST, CSP best practices) and regulatory compliance.
30	Enforce strict access controls, least privilege principles, and two-factor authentication to prevent unauthorized access to sensitive data and system resources.	The RFD proposed solution begins with a principle of least privilege and grants only access that is required, and removes that access when it is no longer needed. Audit trails are created and protected for all data access. 2FA will be provisioned and enforced.
	Training and support infrastructure	
31	Develop comprehensive user training materials including guides, tutorials, and interactive modules to onboard users effectively and promote system proficiency.	RFD will produce user guides, tutorials and video trainings.
32	Establish a dedicated support portal with knowledge base articles, FAQs, and ticketing systems for administrators to address user inquiries and issues promptly.	RFD proposed that FAQ's be built into the application to allow for quick access, we also propose a contact us feature to satisfy the requirement to address user inquiries. If a ticketing system is required RFD recommends that Jira by Atlassian be used.
	Service Level Agreements (SLAs) definition	
33	Define SLAs with clear metrics for system availability, response times, resolution times, and uptime guarantees.	RFD will deliver a high availability system that will exceed 99.9 % up time excluding planned maintenance or other planned outages. If an instance occurs where uptime falls below 99.9% and the cloud provider is at fault RFD will return any credits or compensation to the state of Oklahoma. For example, if the Azure Compute SLA of 99.9% uptime is not met, customers may be eligible for a 10% service credit if the uptime falls between 99.0% and 99.9%, a 20% credit if it falls between 98.0% and 99.0%, and so on.

34	Establish escalation procedures, service credits, and penalties for SLA violations to incentivize adherence to service commitments.	RFD will deliver a high availability system that will exceed 99.9 % up time excluding planned maintenance or other planned outages. If an instance occurs where uptime falls below 99.9% and the cloud provider is at fault RFD will return any credits or compensation to the state of Oklahoma. For example, if the Azure Compute SLA of 99.9% uptime is not met, customers may be eligible for a 10% service credit if the uptime falls between 99.0% and 99.9%, a 20% credit if it falls between 98.0% and 99.0%, and so on.
	Accessibility compliance	
35	Ensure compliance with accessibility standards such as WCAG to make the system accessible to users with disabilities.	RFD takes accessibility very seriously, we use a variety of tools during development and test to ensure that code meets WCAG standards including screen readers and scanning tools such as Axe.
36	Conduct accessibility audits and usability testing with diverse user groups to identify and address accessibility barriers effectively.	RFD will work with the state to identify users that can assist with this testing.

Oklahoma Ethics Commission Political Finance System
Vendor Name: RFD & Associates, Inc.

Pricing Exhibit #2

System	Unit of Measure	List Unit Price	Percent off List	Oklahoma Price	BAFO Price
Software Subscription: See Production Support line item.	N/A	N/A	N/A	N/A	N/A
Hosting: ***We estimated $50,000/year in pass-through Hosting costs. This will not be a profit center for RFD. RFD can manage hosting and pass costs through to OMES.*** ***Estimate is restored to $50,000 with shift away from using OK hossting contract and environments*** ***Includes:*** ***- Leverage OMES OnBase licenses*** ***- Leverage OMES APM/Enterprise Observability licenses (Dynatrace, Elastic, or any APM tool OMES has licenses for)***	Incurred cost	per hosting provider contract for State of Oklahoma	per hosting provider contract for State of Oklahoma	$ 50,000.00	***$50,000.00***
Third-party services and software license costs: ***We estimated $30,000/year in pass-through third party services and software costs. This will not be a profit center for RFD.*** ***Includes:*** ***- Annual penetration testing services*** ***- e-signature software*** ***- Business intelligence software*** ***- Security Software*** ***Estimate is restored to $30,000 with shift away from using OK hosting contract and environments. We will leverage OMES licenses as possible to reduce costs.***	Estimated costs	$ 30,000.00	N/A	$ 30,000.00	***$30,000.00***
Migration: Migration is Not-To-Exceed Pricing. RFD agrees to perform up to 600 hours of data migration tasks, to be billed as used.	Hours; 600 Hours	$200/Hr	25%	$ 90,000.00	$ 90,000.00
Training: Training is Not-To-Exceed Pricing. RFD agrees to perform up to 200 hours of user training, to be billed as used.	Hours; 200 Hours	$200/Hr	25%	$ 30,000.00	$ 30,000.00
Professional Services: Our rate to OK for Professional Services not included in other cost categories is $150/hour, which is 25% off our list price. No additional professional services are proposed at this time.	Hours; estimated at 0 Hours	$200/Hr	25%	$ -	$ -

System	Unit of Measure	List Unit Price	Percent off List	Oklahoma Price	BAFO Price
Implementation Costs: Implementation of Firm-Fixed-Price solution. OMES and RFD will both retain IP ownership. ***Six month warranty period*** Implementation Pay Points: - Project Kick-off: 5% - Requirements Sign-Off: 20% - Design Sign-Off: 20% - Start of UAT: 25% - Go-Live: 30%	List price	$ 2,400,000.00	50%	$ 1,200,000.00	*$ 1,100,000.00*
Year 1 production support: ***Annual support amount is reduced to $220,000 annually, and can be reduced to $200,000 contingent on a three-year committment.*** ***Year 1 production support is a year of Full Production Support. It begins six months post go-live (end of warranty period), and includes:*** ***- 200 hours per support year that OK can use for enhancements or other non-maintenance changes to the system. .*** ***- Manage and maintain the solution.*** ***- Manage and maintain cloud infrastructure.*** ***- 24/7 Performance monitoring and enterprise observability.*** ***- Issue tracking.*** ***- Help desk.***	Year	$ 300,000.00	25%	$ 240,000.00	*$ 220,000.00*
Extra Storage: Additional storage is included in hosting costs.	N/A	N/A	N/A	N/A	N/A

Maintenance and Support	Year 2	Year 3	Year 4	Year 5
Full production support, including: ***One year of support for the delivered solution, including:*** ***- Annual support amount is reduced to $220,000 annually, and can be reduced to $200,000 contingent on a three-year committment.*** ***- 200 hours per support year that OK can use for enhancements or other non-maintenance changes to the system. .*** - Manage and maintain the solution. - Manage and maintain cloud infrastructure. - 24/7 Performance monitoring and enterprise observability. - Issue tracking. - Help desk. ***- To be invoiced annually on the anniversary of the beginning of Support Year 1.***	*$ 220,000.00*	*$ 220,000.00*	*$ 220,000.00*	*$ 220,000.00*

System	Unit of Measure	List Unit Price	Percent off List	Oklahoma Price	BAFO Price
Full production support, including: *One year of support for the delivered solution, including:* *- Annual support amount is reduced to $200,000 annually contingent on a three-year committment.* *- 200 hours per support year that OK can use for enhancements or other non-maintenance changes to the system. .* - Manage and maintain the solution. - Manage and maintain cloud infrastructure. - 24/7 Performance monitoring and enterprise observability. - Issue tracking. - Help desk *- To be invoiced annually on the anniversary of the beginning of Support Year 1.*	*$ 200,000.00*	*$ 200,000.00*	*$ 200,000.00*	*$ 200,000.00*	
Hosting: *We have removed our estimate for hosting. During Demo Q&A, it sounded like OMES would prefer to use its existing contracts to provide hosting for this solution.*	*$0.00*	*$0.00*	*$0.00*	*$0.00*	

Pricing should have definitions to fully describe what is included.
Hourly costs are to be Not To Exceed (NTE) pricing.

Production Management and Support Services

Production Management and Support services to include, but not limited to, correction of defects to software, database, and documentation shall be provided. At a minimum, services shall include the following:

Unless otherwise mutually agreed to by the Contracting Entity and Vendor, Vendor shall provide maintenance and production support for the Electronic Filing System to help ensure 24x7 uptime outside of the normal application maintenance windows.

- Maintenance and production support shall be scheduled with the Contracting Entity and should occur outside of standard business hours to minimize disruption to the ability to use the Electronic Filing System.
- Maintenance services for the Contracting Entity shall include applying fixes for identified/reported defects and furnishing routine, scheduled update services that include solution-specific patches, bundles, maintenance packs, and service packs required to maintain the as-implemented security, performance, availability, and functionality of the system.
- Unless otherwise mutually agreed to by Contracting Entity and Vendor, Vendor shall provide on-site, telephone, e-mail, and/or Teams availability Monday through Sunday as necessary and if requested by the Contracting Entity.
- Vendor shall respond to a notification from the Contracting Entity of an issue or defect with the Electronic Filing System in accordance with the criteria stated below in the Support Response Table. The Contracting Entity shall have sole authority in determining the severity and support level of each notification sent to Vendor by the Contracting Entity.

Support Response

Severity	Description	Support Level	Support Response
Critical - High	An incident that results in a critical business impact. This could include loss of service, data loss or corruption, or the inability to complete processing or workflows within the application.	One	Within 2 hours to return initial e-mail or phone call.

Severity	Description	Support Level	Support Response
Non-Critical - Significant	An incident that results in a significant business impact. The system is operational, with workarounds or partial services.	Two	Within 24 hours to return initial e-mail or phone call.
Non-Critical - Low	An incident that results in a low business impact. All core functionality remains operable, but changes are still required.	Three	Within 48 hours to return initial e-mail or phone call.

Additional Vendor Responsibilities

- Be prepared for rapid response times and expedited resolution activities for issues that arise around the Contracting Entity's filing deadlines as determined by the Contracting Entity.
- Respond to requests for assistance in troubleshooting problems, applying fixes, or performing other important maintenance tasks during non-business hours as established by the Support.Response.Table. Responses may be via telephone, e-mail, or Teams, as appropriate. For the purposes of this contract, the Contracting Entity business hours are Monday through Friday, from 8:00 A.M. to 5:00 P.M. Central Time. The Contracting Entity and Vendor will exchange non-business hours contact information.
- Correct verifiable and reproducible errors. The term "error" shall be interpreted to include defects in the system application documented processes, database design, or code defects.
- Provide a web-based defect tracking/reporting system that is available to staff of the Contracting Entity.
- Furnish routine, scheduled update services that include solution-specific patches, bundles, maintenance packs, and service packs required to maintain the as-implemented security, performance, availability, and functionality of the system.
- Coordinate as applicable with the Contracting Entity regarding planned system application maintenance.

- Facilitate efforts by the Contracting Entity to secure and back up application data to ensure business continuity or disaster recovery.
- Assist the Contracting Entity as necessary during hardware or operating system upgrades in order to minimize application interruptions. Hardware and operating system upgrades are the responsibility of the Contracting Entity.
- Participate in scheduled Disaster Recovery exercises with the Contracting Entity.

Attachment F to
STATE OF OKLAHOMA CONTRACT WITH RFD & ASSOCIATES, INC.
RESULTING FROM SOLICITATION NO. EV00000504

Negotiated Exceptions to the Solicitation

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

REQUESTED EXCEPTIONS NOT APPEARING BELOW HAVE BEEN DECLINED BY THE STATE

RFP Section	Exception
Attachment D. State of Oklahoma Information Technology Terms – **Section 1, Definitions.**	Section 1.9 is hereby deleted and replaced in its entirety by the following: 1.9 **Supplier Intellectual Property** means all tangible or intangible items or things, including the Intellectual Property Rights therein, created or developed by Supplier (a) prior to providing any services or Work Product to Customer or 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) 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. Subject to all State and Federal laws, rules, and regulations including but not limited to the Oklahoma Open Records Act, the RFD Batch Processor, RFD CloudFormation Templates, RFD DynaWrap, and RFD Framework, and any improvements or modifications thereto, shall be considered Supplier Intellectual Property.
Attachment D. State of Oklahoma Information Technology Terms –	Section 11 is hereby deleted and replaced in its entirety by the following: Any Work Product relating to the software developed, modified, or customized by the Supplier in accordance with a mutually negotiated statement of work pursuant to this Contract (the "Software Work Product") shall be jointly owned by Supplier and the State such that each party shall own an equal undivided interest in the same together

RFP Section	Exception
Section 11, Ownership Rights.	with all manuals, source code, 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 the exception of Supplier Intellectual Property and any Customer Data. The parties mutually agree that Supplier shall be the sole and exclusive owner of the existing Intellectual Property of Supplier and the Supplier Intellectual Property. With respect to Supplier Intellectual Property, the Supplier grants the State, for no additional consideration, a perpetual, irrevocable, royalty-free license, to use, copy, modify, display, and perform any Supplier Intellectual Property embodied in or delivered to the State in conjunction with the Work Product delivered pursuant to this Contract, solely for the internal business use of the State, and solely as necessary to make full use of the Work Product as contemplated by this Contract. Supplier shall have the exclusive right to submit U.S. and foreign copyright, trademark, and/or patent applications relating to Software Work Product and the State may assist the Supplier and its agents, upon request with consent of the State, in preparing the same. State may sign any such applications, upon request, and deliver them to the Supplier. The Supplier 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 (which does not include Supplier Intellectual Property) may be shared with other publicly funded agencies at the discretion of the State without permission from or additional compensation to the Supplier.
Attachment D. State of Oklahoma Information Technology Terms – **Section 12, Intellectual Property Ownership to Work Product.**	Section 12 is hereby deleted and replaced in its entirety by the following: The following terms apply to ownership and rights related to Intellectual Property: 12.1 As to the Intellectual Property Rights to Work Product between Supplier and Customer (which does not include Supplier Intellectual Property), the parties agree that they shall be jointly owned by Supplier and the State such that each party shall own an equal undivided interest

RFP Section	Exception
	in the same. 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 Each party, upon request and without further consideration from the other party, shall perform any acts that may be deemed reasonably necessary or desirable to evidence more fully the ownership and/or registration of all Intellectual Property Rights in all Work Product to the fullest extent possible including, but not limited to, the execution, acknowledgement and delivery of such further documents in a form reasonably requested. 12.3 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. 12.4 Upon the request of Customer, but in any event upon termination or expiration of this Contract or a statement of work, Supplier shall delete, destroy, or surrender to Customer, at the Customer's request, any Customer confidential information or Customer Data. 12.5 Customer acknowledges and agrees that, as a joint owner of the Work Product, Supplier may use the Work Product in connection with the provision of services to its other customers without the prior written consent of Customer. Supplier acknowledges that Customer retains full ownership of all Customer Data including Non-Public Data. 12.6 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

RFP Section	Exception
	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. 12.7 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. 12.8 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. 12.9 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.

STATEMENT OF WORK (SOW)

Guardian Replacement
Ethics eFile

Oklahoma Office of Management and Enterprise Services,
for the benefit of the Oklahoma Ethics Commission
11/22/2024

EXHIBIT
3

Table of Contents

1. Introduction

This Statement of Work is made Effective as of date of last signature ("Effective Date") between the State of Oklahoma by and through the Oklahoma Ethics Commission ("State") and RFD & Associates, Inc. ("Supplier") and is a Contract Document in connection with the Agency Specific Contract between the parties effective 12/06/2024, to supply a Political Finance software solution to OEC for the benefit of The State of Oklahoma.

2. Background

The project is driven by the urgent need to modernize the state's approach to political finance transparency and accountability. The primary motivation behind this project is to ensure the continuation of efficient and secure data processing and reporting as the current system approaches its End of Life (EOL) and End of Service in June 2025. The project aims to enhance scalability and performance, improve user experience, ensure compliance and security, enable integration, and streamline maintenance and support.

3. Scope

The goal of this SOW is for RFD & Associates, Inc. (RFD) to create and maintain a system for electronic filing, following the requirements documented in Exhibit_1_Specifications.xlsx of the RFO. This includes, but is not limited to, seven (7) example forms provided in the RFO process, electronic signature; administrative functionality for the management of filers, filing events, and performance of related OEC business tasks; storage of filed forms, and public-facing pages for searching filed reports. The resulting system will be used for candidates and committees at the state level, as well as at the local level for candidates and committees using OEC Political Finance forms

Forms provided during the RFO include:

1. COMMITTEE SCHEDULE A—MONETARY CONTRIBUTIONS
2. COMMITTEE SCHEDULE B—TRANSFERS AND OTHER FUNDS RECEIVED
3. COMMITTEE SCHEDULE C—LOANS
4. COMMITTEE SCHEDULE D—IN KIND CONTRIBUTIONS
5. COMMITTEE SCHEDULE E—GENERAL EXPENDITURES
6. COMMITTEE SCHEDULE F—OFFICEHOLDER EXPENSES
7. CANDIDATE COMMITTEE CONTRIBUTIONS AND EXPENDITURES REPORT

4. Deliverables

4.1. The project is comprised of the following deliverables:

System Implementation:
System implementation is divided into the following key phases, each corresponding to a major deliverable:

- **Project Kick-off:** Establishes project objectives, scope, schedules, and roles to ensure alignment among stakeholders.
- **Requirements Sign-Off:** Captures and finalizes detailed system requirements, including functional, technical, and security specifications.
- **Design Sign-Off:** Formal approval of system design, mockups, architecture, and workflows.
- **Start of UAT:** Deploys the system in a test environment for stakeholder validation through User Acceptance Testing (UAT).

- **Go-Live:** Launches the production-ready system, ensuring all components are operational and compliant with project requirements.

Data Migration:	600 hours included in project; additional hours will be invoiced separately
Training:	200 hours included in project; additional hours will be invoiced separately
Hosting:	Will be invoiced as a pass-through expense with no markup.
3rd-party software:	Licenses will be invoiced as a pass-through expense with no markup

4.2. Deliverable Schedule

Del. No.	Deliverable Description	Estimated Due Date
1	Project Kick-off	12/18/24
2	Requirements Sign-Off	2/3/25
3	Design Sign-Off	2/24/25
4	Start of UAT	6/16/25
5	Go-Live	7/1/25
6	Data Migration	6/20/25
7	Training	6/30/25

4.3. Deliverable Acceptance

Deliverables will be provided to OMES for review and acceptance as soon as all associated requirements for the deliverable are completed, as detailed in the Deliverable Pricing section. Each deliverable will be deemed complete when:

- All defined requirements under the deliverable are fulfilled.
- The associated success criteria are met.

OMES will review deliverables and communicate acceptance, or reasons for rejection, within five (5) business days of receipt. If OMES does not provide feedback within five (5) business days, the deliverable will be considered accepted, and the corresponding invoice will be issued.

The Go-Live deliverable will be invoiced no later than thirty (30) days after the completion of User Acceptance Test (UAT), provided all associated requirements are met and OMES has validated successful deployment of the production system.

This acceptance process ensures alignment with project expectations and timely delivery of milestone payments.

4.4. Deliverable Pricing

Deliverable pricing is as documented in RFD's response to the RFO. That pricing is copied here for convenience.

4.5. Deliverable Incentive

Early Completion: Should Supplier complete a Deliverable, including Substantial Completion, ahead of the agreed upon schedule as set out below, the State agrees to pay an early completion fee for early completion of the Deliverable. The values associated with Early Completion are established via the Deliverable Schedule Chart below.

Del. No.	Deliverable Description	Requirements	Success Criteria	Cost
1	Project Kick-off (5% of implementation)	Due Date	12/18/2024	$55,000.00
		Develop Project Charter with objectives, scope, deliverables, and success criteria.	Charter is approved by stakeholders and clearly defines objectives, deliverables, and metrics for success.	
		Confirm Azure AD integration requirements for SSO.	SSO requirements are fully documented, validated by technical teams, and aligned with MS365 infrastructure.	
		Identify stakeholders and their responsibilities in IAM and RBAC processes.	Stakeholders are identified, and roles and decision-making authorities are documented and agreed upon.	
		Outline initial setup for cloud hosting and SaaS deployment.	Cloud hosting setup is defined with dependencies and requirements for scalability and reliability documented.	
		Ensure dependencies for data migration and reporting tools are documented.	Dependencies for all key areas are fully identified and included in the project plan.	
2	Requirements Sign-Off (20% of implementation)	Due Date:	2/3/2025	$220,000.00
		Confirm requirements for compliance with NIST CSF and Oklahoma IT Security Policies.	Security requirements are documented, reviewed, and approved by relevant security teams.	
		Document detailed requirements for: Internal Admin Interface (MS365 RBAC), External Reporting Interface (IAM/forms), and Public Transparency Dashboard.	Requirements are complete, validated with stakeholders, and approved, ensuring no gaps between scope and expectations.	
		Specify public-facing functionality for transparent reporting without login credentials.	Transparent access requirements are aligned with stakeholder needs and address public access without compromising data security.	
		Define encryption requirements for data at rest and in transit.	Encryption protocols meet compliance standards and are validated by security teams.	

Del. No.	Deliverable Description	Requirements	Success Criteria	Cost
		Validate system's role-based permissions structure for data and feature access.	RBAC structure is defined and verified with test cases to confirm accuracy and alignment with user roles.	
		Establish performance monitoring tools to track uptime, latency, and resource utilization.	Monitoring requirements are documented with clear KPIs, ensuring timely identification and resolution of performance issues.	
		Define comprehensive activity logs and audit trails to record all user actions, changes, and data access.	Audit trail requirements are clearly defined, ensuring traceability and compliance with regulatory requirements.	
3	Design Sign-Off (20% of implementation)	Due Date:	2/24/2025	$220,000.00
		Early Completion Incentive	1% of Deliverable Cost per Early Day of completion. Maximum of 10% Incentive	Max of $22,000
		Present mockups or prototypes for interfaces (internal/external) and tooltips/contextual help for public-facing reports.	Mockups and prototypes are approved by stakeholders, ensuring the design meets functional and usability needs.	
		Deliver architecture design to support scalability, fault tolerance, and elastic scaling.	Architecture documentation is reviewed and approved by technical teams for alignment with scalability and reliability goals.	
		Define and present API structures for secure integrations and data exchange.	API documentation includes endpoints, security protocols, and use cases validated with sample integrations.	
		Validate technical requirements for automated compliance tracking and advanced reporting tools.	Compliance tracking and reporting tools are designed and validated against specified requirements.	
		Define audit trail storage and retrieval processes in the system design.	Audit trail storage requirements are documented and reviewed for efficiency and compliance.	

Del. No.	Deliverable Description	Requirements	Success Criteria	Cost
4	Start of UAT (25% of implementation)	Due Date	6/16/2025	$275,000.00
		Deliver the fully configured system in a test environment, including IAM and RBAC setups, functional compliance forms, and reporting tools.	System passes all initial UAT scenarios, ensuring readiness for stakeholder testing.	
		Ensure data migration is completed for the last five years with validation reports.	Data migration is validated for accuracy, completeness, and accessibility, with no critical errors.	
		Conduct usability testing for public-facing tools, including feedback collection mechanisms.	Feedback from usability tests is reviewed, and improvements are implemented to address any issues.	
5	Go-Live (30% of implementation)	Due Date	7/1/2025	$330,000.00
		Early Completion Incentive *Incentive is a percentage of Deliverable Cost per Early Day Range of Deliverable Completion. Maximum of 20% Incentive	1-5 Days: 2.5% 6-10 Days: 5% 11-15 Days: 8% 16-20 Days: 12% 21-25 Days: 16% 26+ Days: 20%	Max of $66,000
		Deploy final production system, ensuring functionality for forms, workflows, and dashboards.	Final system is deployed and meets all functional, security, and performance requirements.	
		Ensure compliance with Oklahoma EITA Act and validate encryption and security standards for production readiness.	Accessibility features are tested and confirmed to meet EITA compliance standards, and security protocols are validated.	
6	Data Migration (600 hours; invoiced as used)	Due Date	6/20/2025	$90,000.00
		Early Completion Incentive *Incentive is a percentage of Deliverable Cost per Early Day Range of Deliverable Completion. Maximum of 19% Incentive	1-5 Days 2% 6-10 Days 5% 11-15 Days 8% 16-20 Days 11% 21-25 days 15% 26-30 days 19%	Max of $17,100
		Migrate last five years of historical data with schema mapping and data cleansing.	Data migration is completed with no errors, and all data is accessible and accurate in the new system.	

Del. No.	Deliverable Description	Requirements	Success Criteria	Cost
		Validate migrated data with test queries to ensure accuracy and accessibility.	Data validation reports confirm accuracy, with no critical issues outstanding.	
		Include metadata and audit trails as part of the migration process.	Metadata and audit trails are reviewed for integrity and completeness in the new system.	
7	Training (200 hours; invoiced as used)	Due Date	6/30/2025	$30,000.00
		Provide comprehensive training materials for internal administrators and external users.	Training materials are approved and meet the needs of administrative and external users.	
		Include inline tips, pop-up explanations, and contextual help features for public-facing tools.	Contextual help features are demonstrated in the public-facing tools, with user feedback confirming clarity and usability.	
		Ensure training sessions cover compliance features, reporting workflows, and troubleshooting common issues.	Training sessions are evaluated by participants, with improvements implemented based on feedback.	

* Go-Live deliverable will be invoiced no later than thirty (30) days after the completion of User Acceptance Test (UAT).

5. Reports and Meetings

i) RFD will provide detailed monthly status reports to both the OMES project manager and Ethics Commission designated Point of Contact (POC). Reports are due within five (5) business days of the end of the month to ensure alignment between OMES and the Ethics Commission.

ii) The monthly progress reports will:
   a. Detail all work performed and completed during the reporting period.
   b. Outline the planned work for the upcoming month or sprint to maintain visibility into the project's timeline and milestones.
   c. Identify any challenges, risks, or outstanding issues encountered, with an explanation of the root cause and a plan for resolution.

iii) For any identified problems, RFD will provide:
   a. A detailed explanation of the cause.
   b. Proposed resolutions and timelines for resolution.
   c. Regular updates on progress until the issue is fully resolved, ensuring no delays to critical deliverables.

iv) RFD will conduct weekly status meetings with the OMES project manager and Ethics Commission POC(s) to review progress, address risks, and confirm alignment with project requirements. Meetings will:
   a. Be scheduled at a mutually agreed-upon time by OMES and the Ethics Commission.
   b. Be conducted via Microsoft Teams or another online platform specified by OMES.

c. Include key updates on deliverables, schedule adherence, and resolution of issues.

6. Service Level Agreement

RFD will follow service levels as documented in the contract.

7. Period of Performance

The implementation period will commence immediately upon contract execution and will continue through the successful Go-Live milestone. The timeline will include:

- Completion of all deliverables outlined in Section 4.
- Alignment with deliverable schedules as specified in Section 4.2 to ensure timely progress and adherence to required dates.

Implementation will commence upon contract execution, and continue through go-live.

8. Invoices

RFD will invoice OEC upon acceptance of each deliverable as specified in Section 4.3. The invoicing details are as follows:

- For **Data Migration** and **Training**, RFD will invoice based on hours expended and submit invoices on a monthly basis, including detailed timesheets and descriptions of work completed.
- For all other deliverables, invoices will reflect the amounts tied to deliverable completion as specified in Section 4.4.

RFD will invoice OEC for each deliverable upon acceptance of the deliverable. For Data Migration and Training, RFD will invoice expended hours on a monthly basis.

9. Agency/Vendor-Furnished Equipment and Work Space

Agency-Furnished Equipment and Resources:

OMES will:

Assist in the integration of the system with Microsoft Azure Active Directory (Azure AD) for authentication and access management.

The Ethics Commission will:

Provide access to necessary stakeholders to facilitate requirements gathering, testing, and approvals.

The Ethics Commission may:

Designate a Project Manager (PM) and Technical Lead to coordinate integration efforts and provide support throughout the implementation.

Vendor-Furnished Equipment and Resources:

RFD will be responsible for providing:

Hosting Services: Fully managed hosting for the Ethics eFile system, ensuring uptime, scalability, and security in compliance with contract service levels.

Development Environments: All necessary hardware, software, and tools required for the development, configuration, testing, and deployment of the system.

Test Environments: Isolated environments for user acceptance testing (UAT) and validation prior to deployment.

Production Environment: Fully operational production environment, configured and hosted by RFD, to support live system operations.

10. Additional Agency Terms and Conditions

10.1. Point of Contact:

Oklahoma Point of Contact:

Ethics Commission:
2300 N. Lincoln Blvd., G-27, Oklahoma City, OK 73105
Office Main Line: 405-521-3451
Primary: Lee Anne Bruce Boone, Executive Director
Office: 405-521-3451 Cell: 405-763-9012
Email: leeanne.bruceboone@ethics.ok.gov
Secondary: Jeremy Rogers, Deputy Director
Office: 405-522-2514
Email: jeremy.rogers@ethics.ok.gov
Subject Matter Expert (SME): Darci Ray, Administrative Programs Manager
Office: 405-522-2510
Email: darci.ray@ethics.ok.gov

OMES:
2401 N. Lincoln Blvd. Oklahoma City, OK 73105
Contract Manager: Jason LaPierre
Office: 405-523-4041
Email: jason.lapierre@omes.ok.gov

Technical Lead: Craig Brooks, Senior Technical Advisor
Office: 405-522-1560
Email: craig.brooks@omes.ok.gov

RFD Points of Contact

Contract: Tom Lynch
3267 Bee Cave Rd., Ste 107-61, Austin, TX 78747
Cell: 512/426/9613
E-mail: tlynch@rfdinc.com

Project: Erik Dietz
3267 Bee Cave Rd., Ste 107-61, Austin, TX 78747
Cell: 845/551-0036
E-mail: edietz@rfdinc.com

11. Signatures

Vendor:

RFD & ASSOCIATES, INC.

By: Scott T. Glover
Scott T. Glover (Jan 3, 2025 09:23 CST) on 01/03/2025

Name: Scott T. Glover

Title: Chief Operating Officer

Customer:

OKLAHOMA ETHICS COMMISSION

By: Lee Anne Bruce Boone
Lee Anne Bruce Boone (Jan 3, 2025 09:39 CST) on 01/03/2025

Name: Lee Anne Bruce Boone

Title: Executive Director

The OMES Chief Information Officer is signing solely to approve the Contract pursuant to 62 O.S., § 34.11.1 concerning procurement of Information Technology and/or Telecommunications.

By: Aleta Seaman
Aleta Seaman (Jan 3, 2025 09:51 CST) on 01/03/2025

Name: Aleta Seaman

Title: Interim CIO

<End>