

MASTER SERVICES AGREEMENT

THIS MASTER SERVICES AGREEMENT (“Agreement”) is made between the **CITY AND COUNTY OF DENVER**, a municipal corporation of the State of Colorado (the “City”), and **ZIVARO, INC.**, a Colorado corporation, whose address is 3900 E. Mexico Avenue, Suite 1000, Denver, CO 80210 (“Contractor”), individually a “Party” and jointly “the Parties.”

RECITALS

WHEREAS, the City is entering into this Agreement pursuant to a Participating Addendum to NASPO ValuePoint Cloud Solutions administered by the State of Utah with Zivaro, Inc., Master Agreement No. AR3102 and the State of Colorado Contract# 141379, for use by the City and County of Denver pursuant to D.R.M.C. §20-64.5. The terms of this Agreement take precedence over any conflicting terms and conditions in the Participating Addendum.

NOW, THEREFORE, in consideration of the mutual covenants and agreements hereinafter set forth and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the City and Contractor incorporate the recitals set forth above agree as follows:

- 1. DEFINITIONS.** Whenever used herein, any schedules, exhibits, order forms, or addenda to this Agreement, the following terms shall have the meanings assigned below unless otherwise defined therein. Other capitalized terms used in this Agreement are defined in the context in which they are used.
 - 1.1. “**Acceptance**” means the Deliverable demonstrates to the City's reasonable satisfaction that the Deliverable conforms to and operates in all material respects according to the Acceptance Criteria, and if required, has successfully completed Acceptance Testing in all material respects, and for Deliverables not requiring Acceptance Testing that the Deliverable reasonably conforms in all material respects to the Acceptance Criteria or the City's requirements.
 - 1.2. “**Acceptance Certificate**” means a written instrument by which the City promptly notifies Contractor that a Deliverable has been Accepted or Accepted with exceptions, and Acceptance Criteria have been met or waived, in whole or in part.
 - 1.3. “**Acceptance Criteria**” means functionality and performance requirements determined by the City and set forth on the Order Form for the applicable Product or Service, based upon the Specifications, which must be satisfied prior to the City's Acceptance of a Deliverable, or the System. The City and Contractor shall agree upon written Acceptance Criteria in the Order Form for the applicable Product or Service.

- 1.4. "**Acceptance Date**" means the date on which the City issues an Acceptance Certificate for the System or a Deliverable.
- 1.5. "**Acceptance Test**" means the evaluation and testing method, procedures, or both, that are set forth in the Order Form for the applicable Product or Service and are used to determine whether or not the System or a Deliverable requiring Acceptance Testing performs in accordance with the Acceptance Criteria.
- 1.6. "**City Data**" means all information, whether in oral or written (including electronic) form, created by or in any way originating with the City and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by or in any way originating with the City, in the course of using and configuring the Services provided under this Agreement, and includes all records relating to the City's use of Contractor Services. City Data also includes Confidential Information disclosed to Contractor.
- 1.7. "**Confidential Information**" means all records or data that is disclosed in written, graphic or machine recognizable form and is marked, designated, labeled or identified at the time of disclosure as being confidential or its equivalent, or, if the information is in verbal form, it is identified as confidential or proprietary at the time of disclosure and is confirmed in writing within thirty (30) Calendar Days of the disclosure and is not subject to disclosure under CORA. Confidential Information shall include, but is not limited to, PII, PHI, PCI, federal or state tax information ("Tax Information"), Criminal Justice Information (CJI), personnel records, financial, statistical, personnel, human resources data or Personally Identifiable Information and/or Personal Information as described in the C.R.S 24-73-101, *et seq*; attorney/client privileged communications; information which is exempt per federal laws (including but not limited to copyright or HIPPA), all of which is not subject to disclosure under CORA. Confidential Information does not include information which: (a) is public or becomes public through no breach of the confidentiality obligations herein; (b) is disclosed by the party that has received Confidential Information (the "Receiving Party") with the prior written approval of the other party; (c) was known by the Receiving Party at the time of disclosure; (d) was developed independently by the Receiving Party without use of the Confidential Information; (e) becomes known to the Receiving Party from a source other than the disclosing party through lawful means; (f) is disclosed by the disclosing party to others without confidentiality obligations; or (g) is required by law to be disclosed.
- 1.8. "**CORA**" means the Colorado Open Records Act, §§ 24-72-200.1, *et seq.*, C.R.S.

- 1.9. **“Data Incident”** means any accidental or deliberate event that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of any communications or information resources of the City. Data Incidents include, without limitation (i) successful attempts to gain unauthorized access to a City system or the City information regardless of where such information is located; (ii) unwanted disruption or denial of service; (iii) the unauthorized use of a City system for the processing or storage of data; or (iv) changes to the City system hardware, firmware, or software characteristics without the City’s knowledge, instruction, or consent. It shall also include any actual or reasonably suspected unauthorized access to or acquisition of computerized City Data that compromises the security, confidentiality, or integrity of City Data, or the ability of the City to access City Data.
- 1.10. **“Deliverable”** means the Products or Services or documents or tangible work products described in an Order Form to be provided to the City by Contractor or the outcome to be achieved or output to be provided, in the form of a tangible object or software that is produced as a result of Contractor’s work that is intended to be delivered to the City by Contractor under this Agreement.
- 1.11. **“Documentation”** means, collectively: (a) all materials published or otherwise made available to the City by Contractor that relate to the functional, operational and/or performance capabilities of the Services; (b) all user, operator, system administration, technical, support and other manuals and all other materials published or otherwise made available by Contractor, including marketing materials that describe the functional, operational and/or performance capabilities of the Services; (c) any Requests for Information and/or Requests for Proposals (or documents of similar effect) issued by the City, and the responses thereto from Contractor, and any document which purports to update or revise any of the foregoing; and (d) the results of any Contractor “Use Cases Presentation,” “Proof of Concept” or similar type presentations or tests provided by Contractor to the City or as required to be produced by Contractor subject to the terms of this Agreement.
- 1.12. **“Downtime”** means any period of time of any duration that the Services are not made available by Contractor to the City for any reason, including scheduled maintenance or Enhancements.
- 1.13. **“Effective Date”** means the date on which this Agreement is fully approved and signed by the City as shown on the Signature Page for this Agreement. The Effective Date for Services may be set out in an Order Form or similar exhibit.
- 1.14. **“Enhancements”** means any improvements, modifications, upgrades, updates, fixes, revisions and/or expansions to the Services that Contractor may develop or acquire and incorporate into its

standard version of the Services or which Contractor has elected to make generally available to its customers.

- 1.15. "**Equipment**" means any hardware, machinery, device, tool, computer, computer component, computer system, including add-ons, or peripherals of tangible form together with the necessary supplies for upkeep and maintenance, and other apparatus, to be provided to the City by Contractor under this Agreement.
- 1.16. "**Error**" means any defect, problem, condition, bug, or other partial or complete inability of a Product to operate in accordance with the applicable Specifications.
- 1.17. "**Intellectual Property Rights**" includes without limitation all right, title, and interest in and to all (a) Patent and all filed, pending, or potential applications for Patent, including any reissue, reexamination, division, continuation, or continuation in part applications throughout the world now or hereafter filed; (b) trade secret rights and equivalent rights arising under the common law, state law, and federal law; (c) copyrights, other literary property or authors rights, whether or not protected by copyright or as a mask work, under common law, state law, and federal law; and (d) proprietary indicia, trademarks, trade names, symbols, logos, and/or brand names under common law, state law, and federal law.
- 1.18. "**Order Form**" means a quote in the form attached hereto as an exhibit, setting forth certain Products and/or Services to be provided pursuant to this Agreement. Any reference to an "Order Form" in this Agreement includes Products and/or Services purchased by the City pursuant to Contractor's online ordering process. An Order Form can also be a statement of work or scope of work if attached to this Agreement.
- 1.19. "**PCI**" means payment card information including any data related to credit card holders' names, credit card numbers, or other credit card information as may be protected by state or federal law.
- 1.20. "**PII**" means personally identifiable information including, without limitation, any information maintained by the City about an individual that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records. PII includes, but is not limited to, all information defined as personally identifiable information in §§ 24-72-501 and 24-73-101, C.R.S.
- 1.21. "**PHI**" means any protected health information, including, without limitation any information whether oral or recorded in any form or medium: (i) that relates to the past, present, or future physical or mental condition of an individual; the provision of health care to an individual; or the

past, present, or future payment for the provision of health care to an individual; and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. PHI includes, but is not limited to, any information defined as Individually Identifiable Health Information by the federal Health Insurance Portability and Accountability Act. If this Agreement involves the transmission of PHI a separate Business Associates Agreement will become a part of this Agreement.

- 1.22. "**Product(s)**" means software, Equipment, and supplies delivered, or to be delivered, pursuant to an Order Form.
- 1.23. "**Protected Information**" includes, but is not limited to, personally-identifiable information, student records, protected health information, criminal justice information or individual financial information and other data defined under § 24-72-101 *et seq.*, and personal information that is subject to local, state or federal statute, regulatory oversight or industry standard restricting the use and disclosure of such information. The loss of such Protected Information would constitute a direct damage to the City.
- 1.24. "**Services**" means Contractor's computing solutions, provided to the City pursuant to this Agreement, that provide the functionality and/or produce the results described in the Documentation, including without limitation all Enhancements thereto and all interfaces.
- 1.25. "**Service Level Agreement(s)**" mean the provisions set forth on Exhibit A attached hereto, which are incorporated into this Agreement by this reference.
- 1.26. "**Specifications**" means the most current cumulative statement of capabilities, functionality, and performance requirements for the Products or Services as set out in the Acceptance Criteria, Order Forms, Documentation, Contractor's representations, Contractor's proposal, and the City's Request for Proposals.
- 1.27. "**Subcontractor**" means any third party engaged by Contractor to aid in performance of the work or the Service. Contractor shall provide to the City upon request a list of Subcontractors providing material services to the Service.
- 1.28. "**System**" means the operational combination of all Products and Services to be provided by Contractor to the City under this Agreement.
- 1.29. "**Third Party**" means persons, corporations and entities other than Contractor, the City or any of their employees, contractors or agents.
- 1.30. "**Third-Party Host**" means the entity where the physical location of the server(s) of the

Contractor's software resides.

2. RIGHTS AND LICENSE IN AND TO DATA

- 2.1. The Parties agree that as between them, all rights in and to City Data shall remain the exclusive property of the City, and Contractor has a limited, nonexclusive license to access and use City Data as provided in this Agreement solely for the purpose of performing its obligations hereunder.
- 2.2. All City Data created and/or processed by the Service is and shall remain the property of the City and shall in no way become attached to the Service, nor shall Contractor have any rights in or to the City Data without the express written permission of the City and may not include Protected Information.
- 2.3. This Agreement does not give a party any rights, implied or otherwise, to the other's data, content, or intellectual property, except as expressly stated in the Agreement.
- 2.4. The City retains the right to use the Service to access and retrieve data stored on Contractor's Service infrastructure at any time during the term of this Agreement at its sole discretion.

3. DATA PRIVACY

- 3.1. Contractor will use City Data only for the purpose of fulfilling its duties under this Agreement and for the City's sole benefit and will not share City Data with or disclose it to any Third Party without the prior written consent of the City or as otherwise required by law. By way of illustration and not of limitation, Contractor will not use City Data for Contractor's own benefit and, in particular, will not engage in "data mining" of City Data or communications, whether through automated or human means, except as specifically and expressly required by law or authorized in writing by the City.
- 3.2. Contractor will provide access to City Data only to those Contractor employees, contractors and Subcontractors ("Contractor Staff") who need to access City Data to fulfill Contractor's obligations under this Agreement. Contractor will ensure that, prior to being granted access to City Data, Contractor Staff who perform work under this Agreement have all undergone and passed criminal background screenings; have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all data protection provisions of this Agreement; and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of City Data they will be handling.
- 3.3. If Contractor receives Protected Information of a Colorado resident under this Agreement, Contractor shall implement and maintain reasonable written security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of Contractor's business and its operations. Unless Contractor agrees to provide its own security

protections for the information it discloses to a third-party service provider, Contractor shall require all its third-party service providers to implement and maintain reasonable written security procedures and practices that are appropriate to the nature of the personal identifying information disclosed and reasonably designed to help protect the personal identifying information subject to this Agreement from unauthorized access, use, modification, disclosure, or destruction. Contractor and its third-party service providers that maintain electronic or paper documents that contain Protected Information under this Agreement shall develop a written policy for the destruction of such records by shredding, erasing, or otherwise modifying the Protected Information to make it unreadable or indecipherable when the records are no longer needed.

3.4. Contractor may provide City Data to its agents, employees, assigns, and Subcontractors as necessary to perform the work under this Agreement, but shall restrict access to Confidential Information to those agents, employees, assigns, and Subcontractors who require access to perform their obligations under this Agreement. Contractor shall ensure all such agents, employees, assigns, and Subcontractors sign, or have signed, agreements containing nondisclosure provisions at least as protective as those in this Agreement, and that the nondisclosure provisions are in force at all times the agent, employee, assign, or Subcontractor has access to any Confidential Information. Contractor shall provide copies of those signed nondisclosure provisions to the City upon execution of the nondisclosure provisions if requested by the City.

4. DATA SECURITY AND INTEGRITY

4.1. All facilities, whether Contractor hosted or Third-Party Hosted, used to store and process City Data will implement and maintain administrative, physical, technical, and procedural safeguards and best practices at a level sufficient to provide the requested Service availability and to secure City Data from unauthorized access, destruction, use, modification, or disclosure appropriate for City Data. Such measures, when applicable due to the presence of Protected Information, include, but are not limited to, all applicable laws, rules, policies, publications, and guidelines including, without limitation: (i) the most recently promulgated IRS Publication 1075 for all Tax Information, (ii) the most recently updated PCI Data Security Standard from the PCI Security Standards Council for all PCI, (iii) the most recently issued version of the U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Security Policy for all CJI, (iv) the Colorado Consumer Protection Act, (v) the Children's Online Privacy Protection Act (COPPA), (vi) the Family Education Rights and Privacy Act (FERPA), (vii) §24-72-101 et seq., (viii) the Telecommunications

Industry Association (TIA) Telecommunications Infrastructure Standard for Data Centers (TIA-942); (ix) the federal Health Insurance Portability and Accountability Act for all PHI and the HIPAA Business Associate Addendum attached to this Agreement, if applicable. Contractor shall submit to the Manager, within fifteen (15) days of the Manager's written request, copies of Contractor's policies and procedures to maintain the confidentiality of protected health information to which Contractor has access, and if applicable, Contractor shall comply with all HIPAA requirements contained herein or attached as an exhibit.

- 4.2. Contractor warrants that all City Data will be encrypted in transmission (including via web interface) and in storage by a mutually agreed upon National Institute of Standards and Technology (NIST) approved strong encryption method and standard.
- 4.3. Contractor shall use industry-standard and up-to-date security tools, technologies and procedures including, but not limited to anti-virus and anti-malware protections and intrusion detection and reporting in providing Services under this Agreement. Contractor shall ensure that any underlying or integrated software employed by the Service is updated on a regular basis and does not pose a threat to the security of the Service.
- 4.4. Contractor shall, and shall cause its Subcontractors, to do all of the following:
 - 4.4.1. Provide physical and logical protection for all hardware, software, applications, and data that meets or exceeds industry standards and the requirements of this Agreement.
 - 4.4.2. Maintain network, system, and application security, which includes, but is not limited to, network firewalls, intrusion detection (host and network), annual security testing, and improvements or enhancements consistent with evolving industry standards.
 - 4.4.3. Comply with State and federal rules and regulations related to overall security, privacy, confidentiality, integrity, availability, and auditing.
 - 4.4.4. Provide that security is not compromised by unauthorized access to workspaces, computers, networks, software, databases, or other physical or electronic environments.
 - 4.4.5. Promptly report all Data Incidents, including Data Incidents that do not result in unauthorized disclosure or loss of data integrity.
 - 4.4.6. Comply with all rules, policies, procedures, and standards issued by the City's Technology Services Security Section.
 - 4.4.7. Subject to Contractor's reasonable access security requirements and upon reasonable prior notice, Contractor shall provide the City with scheduled access for the purpose of inspecting

and monitoring access and use of City Data, maintaining City systems, and evaluating physical and logical security control effectiveness.

4.4.8. Contractor shall perform current background checks in a form reasonably acceptable to the City on all of its respective employees and agents performing services or having access to City Data provided under this Agreement, including any Subcontractors or the employees of Subcontractors. A background check performed within 30 days prior to the date such employee or agent begins performance or obtains access to City Data shall be deemed to be current.

4.4.9. Contractor will provide notice to the security and compliance representative for the City indicating that background checks have been performed. Such notice will inform the City of any action taken in response to such background checks, including any decisions not to take action in response to negative information revealed by a background check.

4.4.10. If Contractor will have access to Tax Information under the Agreement, Contractor shall comply with the background check requirements defined in IRS Publication 1075 and § 24-50-1002, C.R.S.

4.5. If applicable, Contractor shall use, hold, and maintain Confidential and Protected Information in compliance with all applicable laws and regulations only in facilities located within the United States, and shall maintain a secure environment that ensures confidentiality of all Confidential and Protected Information.

4.6. Prior to the Effective Date of this Agreement, Contractor, will at its expense conduct or have conducted the following, and thereafter, Contractor will at its expense conduct or have conducted the following at least once per year, and immediately after any actual or reasonably suspected Data Incident:

4.6.1. A SSAE 16/SOC 2 or other mutually agreed upon audit of Contractor's security policies, procedures and controls;

4.6.2. A quarterly external and internal vulnerability scan of Contractor's systems and facilities, to include public facing websites, that are used in any way to deliver Services under this Agreement. The report must include the vulnerability, age and remediation plan for all issues identified as critical or high;

4.6.3. A formal penetration test, performed by a process and qualified personnel of Contractor's systems and facilities that are used in any way to deliver Services under this Agreement.

- 4.7. Contractor will provide the City the reports or other documentation resulting from the above audits, certifications, scans and tests within seven (7) business days of Contractor's receipt of such results.
- 4.8. Based on the results and recommendations of the above audits, certifications, scans and tests, Contractor will, within thirty (30) calendar days of receipt of such results, promptly modify its security measures to meet its obligations under this Agreement and provide the City with written evidence of remediation.
- 4.9. The City may require, at its expense, that Contractor perform additional audits and tests, the results of which will be provided to the City within seven (7) business days of Contractor's receipt of such results.
- 4.10. Contractor shall protect data against deterioration or degradation of data quality and authenticity, including, but not limited to annual Third Party data integrity audits. Contractor will provide the City the results of the above audits.
- 4.11. Contractor shall maintain a continuous and uninterrupted business continuity and disaster recovery program with respect to its services provided under this agreement. The program shall be designed, in the event of a significant business disruption affecting Contractor, to provide all of the necessary and sufficient capabilities, processes, and procedures to enable Contractor to resume and continue to perform its duties and obligations under this Agreement without undue delay or disruption.
- 4.12. Prior to the Effective Date of this Agreement, the Contractor, will at its own expense conduct or have conducted the following, and thereafter, Contractor will at its own expense conduct or have conducted the following at least once per year:
- 4.12.1. A test of the operability, sufficiency, and completeness of business continuity and disaster recovery program's capabilities, processes, and procedures that are necessary to resume and continue to perform its duties and obligations under this agreement.
 - 4.12.2. Based upon the results and subsequent recommendations of the testing above, Contractor will, within thirty (30) calendar days of receipt of such results and recommendations, promptly modify its capabilities, processes, and procedures to meet its obligations under this Agreement and provide City with written evidence of remediation.
 - 4.12.3. Contractor will provide the City with report summaries or other documentation resulting from above testing of any business continuity and disaster recovery procedures regarding the services provided under this agreement.

4.13. Contractor represents that it is capable, willing, and able to provide all of the necessary and sufficient business continuity and disaster recovery capabilities and functions that are appropriate for it to provide services under this Agreement.

5. RESPONSE TO LEGAL ORDERS, DEMANDS OR REQUESTS FOR DATA

5.1. Except as otherwise expressly prohibited by law, Contractor will:

5.1.1. If required by a court of competent jurisdiction or an administrative body to disclose City Data, Contractor will notify the City in writing immediately upon receiving notice of such requirement and prior to any such disclosure;

5.1.2. Consult with the City regarding its response;

5.1.3. Cooperate with the City's reasonable requests in connection with efforts by City to intervene and quash or modify the legal order, demand or request; and

5.1.4. Upon request, provide the City with a copy of its response.

5.2. If the City receives a subpoena, warrant, or other legal order, demand or request seeking data maintained by Contractor, the City will promptly provide a copy to Contractor. Contractor will supply the City with copies of data required for the City to respond within forty-eight (48) hours after receipt of copy from the City and will cooperate with the City's reasonable requests in connection with its response.

6. DATA INCIDENT RESPONSE

6.1. Contractor shall maintain documented policies and procedures for Data Incident and breach reporting, notification, and mitigation. If Contractor becomes aware of any Data Incident, it shall notify the City immediately and cooperate with the City regarding recovery, remediation, and the necessity to involve law enforcement, as determined by the City. If there is a Data Incident impacting residents of Colorado or any other jurisdiction, Contractor shall cooperate with the City to satisfy notification requirements as currently defined in either federal, state, or local law. Unless Contractor can establish that neither Contractor nor any of its agents, employees, assigns or Subcontractors are the cause or source of the Data Incident, Contractor shall be responsible for the cost of notifying each person who may have been impacted by the Data Incident as required by law. After a Data Incident, Contractor shall take steps to reduce the risk of incurring a similar type of Data Incident in the future as directed by the City, which may include, but is not limited to, developing and implementing a remediation plan that is approved by the City at no additional cost to the City.

- 6.2. Contractor shall report, either orally or in writing, to the City any Data Incident involving City Data, or circumstances that could have resulted in unauthorized access to or disclosure or use of City Data, not authorized by this Agreement or in writing by the City, including any reasonable belief that an unauthorized individual has accessed City Data. Contractor shall make the report to the City immediately upon discovery of the unauthorized disclosure, but in no event more than forty-eight (48) hours after Contractor reasonably believes there has been such unauthorized use or disclosure. Oral reports by Contractor regarding Data Incidents will be reduced to writing and supplied to the City as soon as reasonably practicable, but in no event more than forty-eight (48) hours after oral report.
- 6.3. Immediately upon becoming aware of any such Data Incident, Contractor shall fully investigate the circumstances, extent and causes of the Data Incident, and report the results to the City and continue to keep the City informed daily of the progress of its investigation until the issue has been effectively resolved.
- 6.4. Contractor's report discussed herein shall identify: (i) the nature of the unauthorized use or disclosure, (ii) the data used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure (if known), (iv) what Contractor has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and (v) what corrective action Contractor has taken or shall take to prevent future similar unauthorized use or disclosure.
- 6.5. Within five (5) calendar days of the date Contractor becomes aware of any such Data Incident, Contractor shall have completed implementation of corrective actions to remedy the Data Incident, restore the City's access to the Services as directed by the City, and prevent further similar unauthorized use or disclosure.
- 6.6. Contractor, at its expense, shall cooperate fully with the City's investigation of and response to any such Data Incident.
- 6.7. Except as otherwise required by law, Contractor will not disclose or otherwise provide notice of the incident directly to any person, regulatory agencies, or other entities, without prior written permission from the City.
- 6.8. Notwithstanding any other provision of this Agreement, and in addition to any other remedies available to the City under law or equity, Contractor will promptly reimburse the City in full for all costs incurred by the City in any investigation, remediation or litigation resulting from any such Data Incident, including but not limited to providing notification to Third Parties whose data were

compromised and to regulatory bodies, law-enforcement agencies or other entities as required by law or contract; establishing and monitoring call center(s), and credit monitoring and/or identity restoration services to assist each person impacted by a Data Incident in such a fashion that, in the City's sole discretion, could lead to identity theft; and the payment of legal fees and expenses, audit costs, fines and penalties, and other fees imposed by regulatory agencies, courts of law, or contracting partners as a result of the Data Incident.

7. DATA RETENTION AND DISPOSAL

- 7.1. Using appropriate and reliable storage media, Contractor will regularly backup data and retain such backup copies consistent with the City's data retention policies.
- 7.2. At the City's election, Contractor will either securely destroy or transmit to the City repository any backup copies of City Data. Contractor will supply the City a certificate indicating the records disposed of, the date disposed of, and the method of disposition used.
- 7.3. Contractor will immediately preserve the state of the data at the time of the request and place a "hold" on data destruction or disposal under its usual records retention policies of records that include data, in response to an oral or written request from the City indicating that those records may be relevant to litigation that the City reasonably anticipates. Oral requests by the City for a hold on record destruction will be reduced to writing and supplied to Contractor for its records as soon as reasonably practicable under the circumstances. The City will promptly coordinate with Contractor regarding the preservation and disposition of these records. Contractor shall continue to preserve the records until further notice by the City.

8. DATA TRANSFER UPON TERMINATION OR EXPIRATION

- 8.1. Upon expiration or earlier termination of this Agreement or any Services provided in this Agreement, Contractor shall accomplish a complete transition of the Services from Contractor to the City or any replacement provider designated solely by the City without any interruption of or adverse impact on the Services or any other services provided by third parties in this Agreement. Contractor shall cooperate fully with the City or such replacement provider and promptly take all steps required to assist in effecting a complete transition of the Services designated by the City. All services related to such transition shall be performed at no additional cost beyond what would be paid for the Services in this Agreement. Contractor shall extend the Agreement monthly if additional time is required beyond the termination of the Agreement, if necessary, to effectuate the transition and the City shall pay a proration of the subscription fee.

8.2. Upon the expiration or termination of this Agreement, Contractor shall return City Data provided to Contractor in a common and readily usable format if requested by the City or destroy City Data and certify to the City that it has done so, as directed by the City. If Contractor is prevented by law or regulation from returning or destroying Confidential Information, Contractor warrants it will guarantee the confidentiality of, and cease to use, such Confidential Information. To the extent that Contractor is requested to perform any services beyond the return of the City's Data in connection with termination assistance, the same shall be performed pursuant to a written statement of work under this Agreement and paid for by the City, applying Contractor's then-current rates for daily/hourly work, as the case may be.

9. SERVICE LEVEL AGREEMENTS; INTERRUPTIONS IN SERVICE; SUSPENSION AND TERMINATION OF SERVICE; CHANGES TO SERVICE. See Exhibit A.

10. COMPLIANCE WITH APPLICABLE LAWS AND CITY POLICIES.

10.1 Contractor will comply with all applicable laws and technology policies in performing the Services under this Agreement. Any Contractor personnel visiting the City's facilities will comply with all applicable City policies regarding access to, use of, and conduct within such facilities. The City will provide copies of such policies to Contractor upon request.

10.2 ADA Website Compliance:

a. Compliance and Testing. All Contractor managed or operated public-facing digital experiences (e.g., websites and webpages) must be compliant with Section 508 of the Rehabilitation Act of 1973 and the WCAG 2.0 Level AA guidelines, as it may be amended (collectively, "Guidelines"). Prior to launching to the public, Contractor shall test all public-facing digital experiences, both manually and in an automated fashion, as applicable, to confirm and maintain compliance with the Guidelines, and then subsequently, no more than once per each term year thereafter. Such manual and automated testing may only be performed by a third party vendor approved by the Department of Justice. The City has a list of approved third party vendors. The City does not warrant the work of any third party vendor. All testing under this section shall be performed by third party vendors at the Contractor's expense.

b. Validation, Review and Remediation. Contractor will notify City when its digital experience is ready for City review and validation. City will then validate, prior to launch and each term year thereafter, to confirm that the digital experience is compliant with the Guidelines. Manual

testing of the Contractor's digital experience will be verified by City with approved vendors and individuals of varying disabilities which shall include individuals who are blind, deaf or hard of hearing, and who have mobility or dexterity limitations. Upon completion of all testing, a review will be performed by the City's web accessibility coordinator to confirm completion of all accessibility requirements. In the event that any deficiencies are discovered in the Contractor's digital experience, City will promptly notify Contractor, and Contractor will remediate prior to launch. A digital experience will not launch until all deficiencies are remediated. All digital experiences must include a statement on the site that the experience is accessible, will maintain accessibility, and will provide a mechanism for users to submit feedback about accessibility issues.

c. In the event that the digital experience fails compliance at any time, Contractor shall bring the digital experience into compliance within ninety (90) days, which may be extended by mutual written agreement of the Parties. Failure to bring the digital experience into compliance for any reason within such time, except as may be mutually extended by the written agreement of the parties, shall be a breach of this Agreement.

10.3 **Criminal Justice Information Services.** As applicable, private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies. All private contractors who perform criminal justice functions shall acknowledge, via signing of the CJIS Security Addendum Certification page, and abide by all aspects of the CJIS Security Addendum. The CJIS Security Addendum is presented in Appendix H. Modifications to the CJIS Security Addendum shall be enacted only by the FBI.

11. WARRANTIES, REPRESENTATIONS AND COVENANTS. Contractor represents and warrants that:

11.1. The Service will conform to applicable specifications, and operate and produce results substantially in accordance with the Documentation and the Exhibits attached hereto, and will be free from deficiencies and defects in materials, workmanship, design and/or performance during the Term of this Agreement;

- 11.2. All technology related services will be performed by qualified personnel in a professional and workmanlike manner, consistent with industry standards;
- 11.3. Contractor has the requisite ownership, rights and licenses to perform its obligations under this Agreement fully as contemplated hereby and to grant to the City all rights with respect to the software and Services free and clear from all liens, adverse claims, encumbrances and interests of any Third Party;
- 11.4. There are no pending or threatened lawsuits, claims, disputes or actions: (i) alleging that any software or service infringes, violates or misappropriates any Third-Party rights; or (ii) adversely affecting any software, service or supplier's ability to perform its obligations hereunder;
- 11.5. The Service will not violate, infringe, or misappropriate any patent, copyright, trademark, trade secret, or other intellectual property or proprietary right of any Third Party;
- 11.6. The software and Services will contain no malicious or disabling code that is intended to damage, destroy or destructively alter software, hardware, systems or data. Contractor's obligations for breach of the Services warranty shall be limited to using its best efforts, at its own expense, to correct or replace that portion of the Services which fails to conform to such warranty, and, if Contractor is unable to correct any breach in the Services Warranty by the date which is sixty (60) calendar days after the City provides notice of such breach, the City may, in its sole discretion, either extend the time for Contractor to cure the breach or terminate this Agreement and receive a full refund of all amounts paid to Contractor under this Agreement.
- 11.7. Disabling Code Warranty. Contractor represents, warrants and agrees that the Services do not contain and the City will not receive from Contractor any virus, worm, trap door, back door, timer, clock, counter or other limiting routine, instruction or design, or other malicious, illicit or similar unrequested code, including surveillance software or routines which may, or is designed to, permit access by any person, or on its own, to erase, or otherwise harm or modify any City system or Data (a "Disabling Code"). In the event a Disabling Code is identified, Contractor shall take all steps necessary, at no additional cost to the City, to: (a) restore and/or reconstruct all City Data lost by the City as a result of Disabling Code; (b) furnish to City a corrected version of the Services without the presence of Disabling Codes; and, (c) as needed, re-implement the Services at no additional cost to the City. This warranty shall remain in full force and effect as long as this Agreement remains in effect.

- 11.8. Third-Party Warranties and Indemnities. Contractor will assign to the City all Third-Party warranties and indemnities that Contractor receives in connection with any products provided to the City. To the extent that Contractor is not permitted to assign any warranties or indemnities through to the City, Contractor agrees to specifically identify and enforce those warranties and indemnities on behalf of the City to the extent Contractor is permitted to do so under the terms of the applicable Third Party agreements.
- 11.9. Contractor warrants it has complied and shall comply with all applicable federal, state, and local laws and regulations of its domicile and wherever performance occurs during the term of this Agreement.
- 11.10. Delivery of Products shall not be construed to represent Acceptance nor shall Delivery of Products relieve Contractor from its responsibility under any representation or warranty. If the City makes a payment for a Product prior to Acceptance, the payment does not grant a waiver of any representation or warranty by Contractor.

12. CONFIDENTIALITY

- 12.1. Contractor shall keep confidential, and cause all Subcontractors to keep confidential, all City Data, unless the City Data is publicly available. Contractor shall not, without prior written approval of the City, use, publish, copy, disclose to any third party, or permit the use by any third party of any City Data, except as otherwise stated in this Agreement, permitted by law, or approved in writing by the City. Contractor shall provide for the security of all Confidential Information in accordance with all applicable laws, rules, policies, publications, and guidelines.
- 12.2. The Receiving Party agrees to exercise the same degree of care and protection with respect to the Confidential Information that it exercises with respect to its own similar Confidential Information and not to directly or indirectly provide, disclose, copy, distribute, republish or otherwise allow any Third Party to have access to any Confidential Information without prior written permission from the disclosing party. However, (a) either party may disclose Confidential Information to its employees and authorized agents who have a need to know; (b) either party may disclose Confidential Information if so required to perform any obligations under this Agreement; and (c) either party may disclose Confidential Information if so required by law (including court order or subpoena). Nothing in this Agreement shall in any way limit the ability of City to comply with any laws or legal process concerning disclosures by public entities. Contractor acknowledges that any responses, materials, correspondence, documents or other information provided to the City are subject to applicable state

and federal law, including the Colorado Open Records Act, and that the release of Confidential Information in compliance with those acts or any other law will not constitute a breach or threatened breach of this Agreement.

12.3. The Receiving Party will inform its employees and officers of the obligations under this Agreement, and all requirements and obligations of the Receiving Party under this Agreement shall survive the expiration or earlier termination of this Agreement. The Receiving Party shall not disclose City Data or Confidential Information to Subcontractors unless such Subcontractors are bound by non-disclosure and confidentiality provisions at least as strict as those contained in this Agreement.

13. COLORADO OPEN RECORDS ACT. The Parties understand that all the material provided or produced under this Agreement, including items marked Proprietary or Confidential, may be subject to the Colorado Open Records Act., § 24-72-201, *et seq.*, C.R.S. In the event of a request to the City for disclosure of such information, the City shall advise Contractor of such request in order to give Contractor the opportunity to object to the disclosure of any of its documents which it marked as proprietary or confidential material. In the event of the filing of a lawsuit to compel such disclosure, the City will tender all such material to the court for judicial determination of the issue of disclosure and Contractor agrees to intervene in such lawsuit to protect and assert its claims of privilege against disclosure of such material or waive the same. Contractor further agrees to defend, indemnify and save and hold harmless the City, its officers, agents and employees, from any claim, damages, expense, loss or costs arising out of Contractor's intervention to protect and assert its claim of privilege against disclosure under this Article including but not limited to, prompt reimbursement to the City of all reasonable attorney fees, costs and damages that the City may incur directly or may be ordered to pay by such court.

14. SOFTWARE AS A SERVICE, SUPPORT AND SERVICES TO BE PERFORMED

14.1. Contractor, under the general direction of, and in coordination with, the City's Chief Information Officer or other designated supervisory personnel (the "Manager") agrees to provide the Services listed on Exhibit A and perform the technology related services described on the attached Exhibit A. The Parties acknowledge that Contractor and the City may work to further define the SOW, in which case that work product ("Follow-Up SOW") will become a part of this Agreement by incorporation. If the Follow-Up SOW materially alters the attached SOW the Parties agree to amend this Agreement in writing.

- 14.2. As the Manager directs, Contractor shall diligently undertake, perform, and complete all of the technology related services and produce all the deliverables set forth on Exhibit A to the City's satisfaction.
- 14.3. Contractor is ready, willing, and able to provide the technology related services and the Services required by this Agreement.
- 14.4. Contractor shall faithfully perform the technology related services in accordance with the standards of care, skill, training, diligence, and judgment provided by highly competent individuals performing services of a similar nature to those described in the Agreement and in accordance with the terms of the Agreement.
- 14.5. User ID Credentials. Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures:
- 14.5.1. Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation);
 - 14.5.2. Account credential lifecycle management from instantiation through revocation;
 - 14.5.3. Account credential and/or identity store minimization or re-use when feasible; and
 - 14.5.4. Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expire able, non-shared authentication secrets).
- 14.6. Vendor Supported Releases. Contractor shall maintain the currency all third-party software used in the development and execution or use of the Service including, but not limited to: all code libraries, frameworks, components, and other products (e.g., Java JRE, code signing certificates, .NET, jQuery plugins, etc.), whether commercial, free, open-source, or closed-source; with third-party vendor approved and supported releases.
- 14.7. Identity Management. The City's Identity and Access Management (IdM) system is an integrated infrastructure solution that enables many of the City's services and online resources to operate more efficiently, effectively, economically and securely. All new and proposed applications must utilize the authentication and authorization functions and components of the IdM. Strong authentication is required for privileged accounts or accounts with access to sensitive information. This technical requirement applies to all solutions, regardless to where the application is hosted.

15. GRANT OF LICENSE; RESTRICTIONS

- 15.1. Contractor hereby grants to the City a right and license to display, perform, and use the Services and use all intellectual property rights necessary to use the Services as authorized.
- 15.2. Title to and ownership of the Service will remain with Contractor. The City will not reverse engineer or reverse compile any part of the Service. The City will not remove, obscure or deface any proprietary notice or legend contained in the Service or Documentation without Contractor's prior written consent.

16. DELIVERY AND ACCEPTANCE

- 16.1. Right to Perform Acceptance Testing. Prior to accepting Deliverables, the City shall have the right to perform Acceptance Testing to evaluate the Deliverable(s) to ensure they meet Acceptance Criteria, if any, set forth on the applicable Order Form or Statement of Work. Contractor shall cooperate with the City in the development of Acceptance Criteria that shall be codified in the applicable Order Form or Statement of Work that will set forth the location, date, and other specifications of the Acceptance Testing, if any. Acceptance Testing may occur in one or more phases, depending on the integration of contingent products, scalability, performance tuning or other measurable features or milestones.
- 16.2. After an Acceptance Test and if at any time the Service does not conform, the City will notify Contractor in writing within sixty (60) days and will specify in reasonable detail the identified failures and possible reasons for failure. Contractor will, at its expense, repair or replace the nonconforming product within fifteen (15) days after receipt of the City's notice of deficiency.
- 16.3. If the City issues an Acceptance Certificate for an "Acceptance with Exception(s)" the City will list the exception(s) and the date for Contractor's correction of the Error(s). If Error(s) are corrected by the listed date(s) the City agrees to commence further Acceptance Testing of the Deliverable or affected portion(s). If the Deliverable passes the Acceptance Tests, the City will issue an Acceptance Certificate.
- 16.4. If a Deliverable fails a second or subsequent Acceptance Test (or in the event of a single Acceptance Test, the Acceptance Test) in no event shall there be an increase to the original price agreed to by the Parties for the Deliverable.
- 16.5. The foregoing procedure will be repeated until the City accepts or finally rejects the Deliverable, in whole or part, in its sole discretion. In the event that the Service does not perform to the City's satisfaction, the City reserves the right to repudiate acceptance. If the City finally rejects the Service, or repudiates acceptance of it, Contractor will refund to the City all fees paid, if any, by the City with respect to the Service.

16.6. If the City is not satisfied with Contractor's performance of the technology related services described in the Statement of Work, the City will so notify Contractor within thirty (30) days after Contractor's performance thereof. Contractor will, at its own expense, re-perform the service within fifteen (15) days after receipt of City's notice of deficiency. The foregoing procedure will be repeated until City accepts or finally rejects the technology related service in its sole discretion. If City finally rejects any technology related service, Contractor will refund to City all fees paid by City with respect to such technology related service.

16.7. Contractor warrants that during the term of this Agreement that the Service and any associated components will not materially diminish during the subscription Term.

17. TERM. The term of the Agreement is from November 1, 2022, through November 1, 2027 (the "Term").

18. COMPENSATION AND PAYMENT

18.1. Fee: The fee for the Services and technology related services is described in the attached Exhibit A (the "Fee"). The Fee shall be paid pursuant to the City's Prompt Payment Ordinance.

18.2. Reimbursement Expenses: The fees specified above include all expenses, and no other expenses shall be separately reimbursed or incurred hereunder for the provision of the Service(s).

18.3. Invoicing: Contractor must submit an invoice which shall include the City contract number, clear identification of the deliverable that has been completed, and other information reasonably requested by the City. Payment on all uncontested amounts shall be made in accordance with the City's Prompt Payment Ordinance.

18.4. Maximum Agreement Liability:

18.4.1. Notwithstanding any other provision of the Agreement, the City's maximum payment obligation will not exceed Seven Million Dollars (\$7,000,000.00) (the "Maximum Agreement Amount"). The City is not obligated to execute an Agreement or any amendments for any further services, including any services performed by Contractor beyond that specifically described in the attached Exhibits. Any services performed beyond those in the attached Exhibits are performed at Contractor's risk and without authorization under the Agreement.

18.4.2. The City's payment obligation, whether direct or contingent, extends only to funds appropriated annually by the Denver City Council, paid into the Treasury of the City, and encumbered for the purpose of the Agreement. The City does not by the Agreement irrevocably pledge present cash reserves for payment or performance in future fiscal years. The Agreement

does not and is not intended to create a multiple-fiscal year direct or indirect debt or financial obligation of the City.

19. STATUS OF CONTRACTOR. Contractor is an independent contractor retained to perform professional or technical services for limited periods of time. Neither Contractor nor any of its employees are employees or officers of the City under Chapter 18 of the Denver Revised Municipal Code, or for any purpose whatsoever.

20. TERMINATION

20.1. The City has the right to terminate the Agreement, or a product under the Agreement, with cause upon written notice effective immediately, and without cause upon twenty (20) days prior written notice to Contractor. However, nothing gives Contractor the right to perform services under the Agreement beyond the time when its services become unsatisfactory to the Manager.

20.2. Notwithstanding the preceding paragraph, the City may terminate the Agreement if Contractor or any of its officers or employees are convicted, plead nolo contendere, enter into a formal agreement in which they admit guilt, enter a plea of guilty or otherwise admit culpability to criminal offenses of bribery, kick backs, collusive bidding, bid-rigging, antitrust, fraud, undue influence, theft, racketeering, extortion or any offense of a similar nature in connection with Contractor's business. Termination for the reasons stated in this paragraph is effective upon receipt of notice.

20.3. Upon termination of the Agreement, with or without cause, Contractor shall have no claim against the City by reason of, or arising out of, incidental or relating to termination, except for compensation for work duly requested and satisfactorily performed as described in the Agreement and shall refund to the City any prepaid cost or expenses.

21. EXAMINATION OF RECORDS AND AUDITS. Any authorized agent of the City, including the City Auditor or his or her representative, has the right to access, and the right to examine, copy and retain copies, at City's election in paper or electronic form, any pertinent books, documents, papers and records related to Contractor's performance pursuant to this Agreement, provision of any goods or services to the City, and any other transactions related to this Agreement. Contractor shall cooperate with City representatives and City representatives shall be granted access to the foregoing documents and information during reasonable business hours and until the latter of three (3) years after the final payment under the Agreement or expiration of the applicable statute of limitations. When conducting an audit of this Agreement, the City Auditor shall be subject to government auditing standards issued by the United States Government Accountability Office by the Comptroller General of the United

States, including with respect to disclosure of information acquired during the course of an audit. No examination of records and audits pursuant to this paragraph shall require Contractor to make disclosures in violation of state or federal privacy laws. Contractor shall at all times comply with D.R.M.C. 20-276.

22. WHEN RIGHTS AND REMEDIES NOT WAIVED. In no event shall any action by either Party hereunder constitute or be construed to be a waiver by the other Party of any breach of covenant or default which may then exist on the part of the Party alleged to be in breach, and the non-breaching Party's action or inaction when any such breach or default shall exist shall not impair or prejudice any right or remedy available to that Party with respect to such breach or default; and no assent, expressed or implied, to any breach of any one or more covenants, provisions or conditions of the Agreement shall be deemed or taken to be a waiver of any other breach.

23. INSURANCE

23.1. General Conditions: Contractor agrees to secure, at or before the time of execution of this Agreement, the following insurance covering all operations, goods or services provided pursuant to this Agreement. Contractor shall keep the required insurance coverage in force at all times during the term of the Agreement, including any extension thereof, and during any warranty period. The required insurance shall be underwritten by an insurer licensed or authorized to do business in Colorado and rated by A.M. Best Company as "A-VIII" or better. Each policy shall require notification to the City in the event any of the required policies be canceled or non-renewed before the expiration date thereof. Such written notice shall be sent to the parties identified in the Notices section of this Agreement. Such notice shall reference the City contract number listed on the signature page of this Agreement. Said notice shall be sent thirty (30) days prior to such cancellation or non-renewal unless due to non-payment of premiums for which notice shall be sent ten (10) days prior. If such written notice is unavailable from the insurer, Contractor shall provide written notice of cancellation, non-renewal and any reduction in coverage to the parties identified in the Notices section by certified mail, return receipt requested within three (3) business days of such notice by its insurer(s) and referencing the City's contract number. Contractor shall be responsible for the payment of any deductible or self-insured retention. The insurance coverages specified in this Agreement are the minimum requirements, and these requirements do not lessen or limit the liability of the Contractor. The Contractor shall maintain, at its own expense, any additional kinds or amounts of insurance that it may deem necessary to cover its obligations and liabilities under this Agreement.

- 23.2. Proof of Insurance: Contractor may not commence services or work relating to this Agreement prior to placement of coverages required under this Agreement. Contractor certifies that the certificate of insurance attached as Exhibit B, preferably an ACORD form, complies with all insurance requirements of this Agreement. The City requests that the City's contract number be referenced on the certificate of insurance. The City's acceptance of a certificate of insurance or other proof of insurance that does not comply with all insurance requirements set forth in this Agreement shall not act as a waiver of Contractor's breach of this Agreement or of any of the City's rights or remedies under this Agreement. The City's Risk Management Office may require additional proof of insurance, including but not limited to policies and endorsements.
- 23.3. Additional Insureds: For Commercial General Liability, Auto Liability and Excess Liability/Umbrella (if required), Contractor and subcontractor's insurer(s) shall include the City and County of Denver, its elected and appointed officials, employees and volunteers as additional insured.
- 23.4. Waiver of Subrogation: For all coverages required under this Agreement, Contractor's insurer shall waive subrogation rights against the City.
- 23.5. Subcontractors and Subconsultants: Contractor shall confirm and document that all subcontractors and subconsultants (including independent contractors, suppliers or other entities providing goods or services required by this Agreement) procure and maintain coverage as approved by the Contractor and appropriate to their respective primary business risks considering the nature and scope of services provided.
- 23.6. Workers' Compensation and Employer's Liability Insurance: Contractor shall maintain the coverage as required by statute for each work location and shall maintain Employer's Liability insurance with limits of \$100,000 per occurrence for each bodily injury claim, \$100,000 per occurrence for each bodily injury caused by disease claim, and \$500,000 aggregate for all bodily injuries caused by disease claims.
- 23.7. Commercial General Liability: Contractor shall maintain a Commercial General Liability insurance policy with minimum limits of \$1,000,000 for each bodily injury and property damage occurrence, \$2,000,000 products and completed operations aggregate (if applicable), and \$2,000,000 policy aggregate.
- 23.8. Automobile Liability: Contractor shall maintain Automobile Liability with minimum limits of \$1,000,000 combined single limit applicable to all owned, hired and non-owned vehicles used in performing services under this Agreement.

23.9. Technology Errors & Omissions including Cyber Liability: Contractor shall maintain Technology Errors and Omissions insurance including cyber liability, network security, privacy liability and product failure coverage with minimum limits of \$1,000,000 per occurrence and \$1,000,000 policy aggregate. The policy shall be kept in force, or a Tail policy placed, for three (3) years.

24. DEFENSE AND INDEMNIFICATION

24.1. Contractor hereby agrees to defend, indemnify, reimburse and hold harmless City, its appointed and elected officials, agents and employees for, from and against all liabilities, claims, judgments, suits or demands for damages to persons or property arising out of, resulting from, or relating to the work performed under this Agreement (“Claims”), unless such Claims have been specifically determined by the trier of fact to be the sole negligence or willful misconduct of the City. This indemnity shall be interpreted in the broadest possible manner to indemnify City for any acts or omissions of Contractor or its subcontractors either passive or active, irrespective of fault, including City’s concurrent negligence whether active or passive, except for the sole negligence or willful misconduct of City.

24.2. Contractor’s duty to defend and indemnify City shall arise at the time written notice of the Claim is first provided to City regardless of whether Claimant has filed suit on the Claim. Contractor’s duty to defend and indemnify City shall arise even if City is the only party sued by claimant and/or claimant alleges that City’s negligence or willful misconduct was the sole cause of claimant’s damages.

24.3. Contractor will defend any and all Claims which may be brought or threatened against City and will pay on behalf of City any expenses incurred by reason of such Claims including, but not limited to, court costs and attorney fees incurred in defending and investigating such Claims or seeking to enforce this indemnity obligation. Such payments on behalf of City shall be in addition to any other legal remedies available to City and shall not be considered City’s exclusive remedy.

24.4. Insurance coverage requirements specified in this Agreement shall in no way lessen or limit the liability of Contractor under the terms of this indemnification obligation. Contractor shall obtain, at its own expense, any additional insurance that it deems necessary for the City’s protection.

24.5. This defense and indemnification obligation shall survive the expiration or termination of this Agreement.

24.6. Contractor shall indemnify, save, and hold harmless the Indemnified Parties, against any and all costs, expenses, claims, damages, liabilities, and other amounts (including attorneys’ fees and costs)

incurred by the Indemnified Parties in relation to any claim that any Deliverable, Service, software, or work product provided by Contractor under this Agreement (collectively, “IP Deliverables”), or the use thereof, infringes a patent, copyright, trademark, trade secret, or any other intellectual property right.

- 25. COLORADO GOVERNMENTAL IMMUNITY ACT.** The Parties hereto understand and agree that the City is relying upon, and has not waived, the monetary limitations and all other rights, immunities and protection provided by the Colorado Governmental Act, § 24-10-101, *et seq.*, C.R.S. (2003).
- 26. TAXES, CHARGES AND PENALTIES.** The City shall not be liable for the payment of taxes, late charges or penalties of any nature other than the compensation stated herein, except for any additional amounts which the City may be required to pay under D.R.M.C. § 20-107 to § 20-115.
- 27. ASSIGNMENT; SUBCONTRACTING.** Contractor shall not voluntarily or involuntarily assign any of its rights or obligations, or subcontract performance obligations, under this Agreement without obtaining the Manager’s prior written consent. Any assignment or subcontracting without such consent will be ineffective and void and shall be cause for termination of this Agreement by the City. The Manager has sole and absolute discretion whether to consent to any assignment or subcontracting, or to terminate the Agreement because of unauthorized assignment or subcontracting. In the event of any subcontracting or unauthorized assignment: (i) Contractor shall remain responsible to the City; and (ii) no contractual relationship shall be created between the City and any sub-consultant, Subcontractor or assign.
- 28. NO THIRD-PARTY BENEFICIARY.** Enforcement of the terms of the Agreement and all rights of action relating to enforcement are strictly reserved to the Parties. Nothing contained in the Agreement gives or allows any claim or right of action to any third person or entity. Any person or entity other than the City or Contractor receiving services or benefits pursuant to the Agreement is an incidental beneficiary only.
- 29. NO AUTHORITY TO BIND CITY TO CONTRACTS.** Contractor lacks any authority to bind the City on any contractual matters. Final approval of all contractual matters that purport to obligate the City must be executed by the City in accordance with the City’s Charter and the Denver Revised Municipal Code.
- 30. AGREEMENT AS COMPLETE INTEGRATION-AMENDMENTS.** Except for the functional requirements provided in response to a request for proposal and/or any subsequent enhancement of

the SOW or other implementation documentation that may be developed after execution of this Agreement, the Agreement is the complete integration of all understandings between the Parties as to the subject matter of the Agreement. No prior, contemporaneous or subsequent addition, deletion, or other modification has any force or effect, unless embodied in the Agreement in writing. No oral representation by any officer or employee of the City at variance with the terms of the Agreement or any written amendment to the Agreement will have any force or effect or bind the City.

31. SEVERABILITY. Except for the provisions of the Agreement requiring appropriation of funds and limiting the total amount payable by the City, if a court of competent jurisdiction finds any provision of the Agreement or any portion of it to be invalid, illegal, or unenforceable, the validity of the remaining portions or provisions will not be affected, if the intent of the Parties can be fulfilled.

32. CONFLICT OF INTEREST

32.1. No employee of the City shall have any personal or beneficial interest in the services or property described in the Agreement. Contractor shall not hire, or contract for services with, any employee or officer of the City that would be in violation of the City's Code of Ethics, D.R.M.C. § 2-51, *et seq.* or the Charter §§ 1.2.8, 1.2.9, and 1.2.12.

32.2. Contractor shall not engage in any transaction, activity or conduct that would result in a conflict of interest under the Agreement. Contractor represents that it has disclosed any and all current or potential conflicts of interest. A conflict of interest shall include transactions, activities or conduct that would affect the judgment, actions or work of Contractor by placing Contractor's own interests, or the interests of any party with whom Contractor has a contractual arrangement, in conflict with those of the City. The City, in its sole discretion, will determine the existence of a conflict of interest and may terminate the Agreement in the event it determines a conflict exists, after it has given Contractor written notice describing the conflict.

33. NOTICES. All notices required by the terms of the Agreement must be hand delivered, sent by overnight courier service, mailed by certified mail, return receipt requested, or mailed via United States mail, postage prepaid, if to Contractor at the address first above written, and if to the City at:

Chief Information Officer or Designee
201 West Colfax Avenue, Dept. 301
Denver, Colorado 80202

With a copy of any such notice to:

Denver City Attorney's Office

1437 Bannock St., Room 353
Denver, Colorado 80202

Notices hand delivered or sent by overnight courier are effective upon delivery. Notices sent by certified mail are effective upon receipt. Notices sent by mail are effective upon deposit with the U.S. Postal Service. The Parties may designate substitute addresses where or persons to whom notices are to be mailed or delivered. However, these substitutions will not become effective until actual receipt of written notification.

- 34. DISPUTES.** All disputes between the City and Contractor arising out of or regarding the Agreement will be resolved by administrative hearing pursuant to the procedure established by D.R.M.C. § 56-106(b)-(f). For the purposes of that administrative procedure, the City official rendering a final determination shall be the Manager as defined in this Agreement.
- 35. GOVERNING LAW; VENUE.** The Agreement will be construed and enforced in accordance with applicable federal law, the laws of the State of Colorado, and the Charter, Revised Municipal Code, ordinances, regulations and Executive Orders of the City and County of Denver, which are expressly incorporated into the Agreement. Unless otherwise specified, any reference to statutes, laws, regulations, charter or code provisions, ordinances, executive orders, or related memoranda, includes amendments or supplements to same. Venue for any legal action relating to the Agreement will be in the District Court of the State of Colorado, Second Judicial District. Contractor shall perform or cause to be performed all services in full compliance with all applicable laws, rules, regulations and codes of the United States, the State of Colorado; and with the Charter, ordinances, rules, regulations and Executive Orders of the City and County of Denver.
- 36. NO DISCRIMINATION IN EMPLOYMENT.** In connection with the performance of work under the Agreement, the Contractor may not refuse to hire, discharge, promote, demote, or discriminate in matters of compensation against any person otherwise qualified, solely because of race, color, religion, national origin, ethnicity, citizenship, immigration status, gender, age, sexual orientation, gender identity, gender expression, marital status, source of income, military status, protective hairstyle, or disability. The Contractor shall insert the foregoing provision in all subcontracts.
- 37. USE, POSSESSION OR SALE OF ALCOHOL OR DRUGS.** Contractor shall cooperate and comply with the provisions of Executive Order 94 and Attachment A thereto concerning the use, possession or sale of alcohol or drugs. Violation of these provisions or refusal to cooperate with

implementation of the policy can result in the City barring Contractor from City facilities or participating in City operations.

- 38. LEGAL AUTHORITY.** Contractor represents and warrants that it possesses the legal authority, pursuant to any proper, appropriate and official motion, resolution or action passed or taken, to enter into the Agreement. Each person signing and executing the Agreement on behalf of Contractor represents and warrants that he has been fully authorized by Contractor to execute the Agreement on behalf of Contractor and to validly and legally bind Contractor to all the terms, performances and provisions of the Agreement. The City shall have the right, in its sole discretion, to either temporarily suspend or permanently terminate the Agreement if there is a dispute as to the legal authority of either Contractor or the person signing the Agreement to enter into the Agreement.
- 39. NO CONSTRUCTION AGAINST DRAFTING PARTY.** The Parties and their respective counsel have had the opportunity to review the Agreement, and the Agreement will not be construed against any party merely because any provisions of the Agreement were prepared by a particular party.
- 40. ORDER OF PRECEDENCE.** In the event of any conflicts between the language of the Agreement and the exhibits, the language of the Agreement controls.
- 41. SURVIVAL OF CERTAIN PROVISIONS.** The terms of the Agreement and any exhibits and attachments that by reasonable implication contemplate continued performance, rights, or compliance beyond expiration or termination of the Agreement survive the Agreement and will continue to be enforceable. Without limiting the generality of this provision, Contractor's obligations to provide insurance and to indemnify the City will survive for a period equal to any and all relevant statutes of limitation, plus the time necessary to fully resolve any claims, matters, or actions begun within that period.
- 42. INUREMENT.** The rights and obligations of the Parties herein set forth shall inure to the benefit of and be binding upon the Parties hereto and their respective successors and assigns permitted under this Agreement.
- 43. TIME IS OF THE ESSENCE.** The Parties agree that in the performance of the terms, conditions, and requirements of this Agreement, time is of the essence.
- 44. FORCE MAJEURE.** Neither party shall be responsible for failure to fulfill its obligations hereunder or liable for damages resulting from delay in performance as a result of war, fire, strike, riot or insurrection, natural disaster, unreasonable delay of carriers, governmental order or regulation, complete or partial shutdown of plant, unreasonable unavailability of equipment or software from

suppliers, default of a Subcontractor or vendor (if such default arises out of causes beyond their reasonable control), the actions or omissions of the other party or its officers, directors, employees, agents, Contractors or elected officials and/or other substantially similar occurrences beyond the party's reasonable control ("Excusable Delay") herein. In the event of any such Excusable Delay, time for performance shall be extended for a period of time as may be reasonably necessary to compensate for such delay.

- 45. PARAGRAPH HEADINGS.** The captions and headings set forth herein are for convenience of reference only and shall not be construed to define or limit the terms and provisions hereof.
- 46. CITY EXECUTION OF AGREEMENT.** This Agreement is expressly subject to and shall not be or become effective or binding on the City until it has been fully executed by all signatories of the City and County of Denver.
- 47. COUNTERPARTS OF THIS AGREEMENT.** This Agreement may be executed in counterparts, each of which shall be deemed to be an original of this Agreement.
- 48. ELECTRONIC SIGNATURES AND ELECTRONIC RECORDS.** Contractor consents to the use of electronic signatures by the City. The Agreement, and any other documents requiring a signature hereunder, may be signed electronically by the City in the manner specified by the City. The Parties agree not to deny the legal effect or enforceability of the Agreement solely because it is in electronic form or because an electronic record was used in its formation. The Parties agree not to object to the admissibility of the Agreement in the form of an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the ground that it is an electronic record or electronic signature or that it is not in its original form or is not an original.
- 49. ADVERTISING AND PUBLIC DISCLOSURE.** Contractor shall not include any reference to the Agreement or to services performed pursuant to the Agreement in any of Contractor's advertising or public relations materials without first obtaining the written approval of the Manager. Any oral presentation or written materials related to services performed under the Agreement will be limited to services that have been accepted by the City. Contractor shall notify the Manager in advance of the date and time of any presentation. Nothing in this provision precludes the transmittal of any information to City officials.
- 50. COMPLIANCE FOR IN-SCOPE SERVICES.** Contractor covenants and agrees to comply with all information security and privacy obligations imposed by any federal, state, or local statute or

regulation, or by any industry standards or guidelines, as applicable based on the classification of the data relevant to Contractor's performance under the Agreement. Such obligations may arise from:

Health Information Portability and Accountability Act (HIPAA)

IRS Publication 1075

Payment Card Industry Data Security Standard (PCI-DSS)

FBI Criminal Justice Information Service Security Addendum

CMS Minimum Acceptable Risk Standards for Exchanges and further covenants and agrees to maintain compliance with the same when appropriate for the data and Services provided under the Agreement. Contractor further agrees to exercise reasonable due diligence to ensure that all of its service providers, agents, business partners, contractors, Subcontractors and any person or entity that may have access to City Data under this Agreement maintain compliance with and comply in full with the terms and conditions set out in this Section. Notwithstanding Force Majeure, the respective processing, handling, and security standards and guidelines referenced by this section may be revised or changed from time to time or City Data may be utilized within the Services that change the compliance requirements. If compliance requirements change, Contractor and the City shall collaborate in good faith and use all reasonable efforts to become or remain compliant as necessary under this section. If compliance is required or statutory and no reasonable efforts are available, the City at its discretion may terminate the agreement for cause.

51. ON-LINE AGREEMENT DISCLAIMER. Notwithstanding anything to the contrary herein, the City shall not be subject to any provision included in any terms, conditions, or agreements appearing on Contractor's or a Subcontractor's website or any provision incorporated into any click-through or online agreements related to the work unless that provision is specifically referenced in this Agreement.

52. PROHIBITED TERMS. Any term included in this Agreement that requires the City to indemnify or hold Contractor harmless; requires the City to agree to binding arbitration; limits Contractor's liability for damages resulting from death, bodily injury, or damage to tangible property; or that conflicts with this provision in any way shall be void ab initio. Nothing in this Agreement shall be construed as a waiver of any provision of § 24-106-109 C.R.S.

53. PCI DSS COMPLIANCE [ONLY FOR CREDIT CARD INTERFACE]

53.1. If Contractor is directly involved in the processing, storage, or transmission of cardholder data on behalf of the City as part of this Agreement, this Section applies. Any Contractor who

provides or has access to software, systems, hardware, or devices which process and/or interact with payment card information or payment cardholder data must be compliant with the current version of the Payment Card Industry Data Security Standard (PCI DSS).

53.2. Contractor covenants and agrees to comply with Visa's Cardholder Information Security Program (CISP), MasterCard's Site Data Protection Rules (SDP), and with all other credit card association or National Automated Clearing House Association (NACHA) rules or rules of member organizations ("Association"), and further covenants and agrees to maintain compliance with the PCI DSS, SDP, and (where applicable) the Payment Application Data Security Standard (PA-DSS) (collectively, the "Security Guidelines"). Contractor represents and warrants that all of the hardware and software components utilized for the City or used under this Agreement is now, and will be PCI DSS compliant during the term of this Agreement. All service providers that Contractor uses under the Agreement must be recognized by Visa as PCI DSS compliant. Contractor further agrees to exercise reasonable due diligence to ensure that all of its service providers (as defined by the PCI Security Council), agents, business partners, contractors, Subcontractors and any person or entity that may have access to credit card information under this Agreement maintain compliance with the Security Guidelines and comply in full with the terms and conditions set out in this Section. Contractor further certifies that the equipment, as described herein, will be deployed in a manner that meets or exceeds the PA DSS and/or PCI certification and will be deployed on a network that meets or exceeds PCI standards. Contractor shall demonstrate its compliance with PCI DSS by annually providing the City an executed Attestation of Compliance (AOC). Contractor must provide verification to the City, prior to start up and ongoing annually during the term of this Agreement, that all modules of Contractor's system(s) that interface with or utilize credit card information in any manner or form of collection are PCI DSS compliant. If the Contractor is a service provider involved in the processing, storage or transmission of cardholder data or sensitive authentication data (collectively "Data Handling") on behalf of the City that would result in Data Handling being included in the City's PCI scope through connected software or components, then the Contractor must provide a PCI Responsibility Matrix ("Matrix") to be attached to this Agreement as an exhibit. The Matrix must identify where responsibility resides for each PCI control requirement, whether it be with the Contractor, the City or shared by both. Any PCI control requirements that do not apply should be indicated along with any pertinent notes.

- 53.3. Contractor shall not retain or store CAV2/CVC2/CVV2/CID or such data prohibited by PCI DSS subsequent to authorization of a credit card transaction, shall prohibit disclosure of any and all cardholder information, and in the event of a compromise of credit card information of any kind, Contractor shall notify the City in writing consistent with the Data Incident response notification requirements of this Agreement, and shall provide, at Contractor's sole expense, all necessary and appropriate notification to parties and persons affected by such disclosure and compromise.
- 53.4. If any Association requires an audit of Contractor or any of Contractor's Service Providers, agents, business partners, contractors or Subcontractors due to a data security compromise event related to this Agreement, Contractor agrees to cooperate with such audit. If as a result of an audit of the City it is determined that any loss of information is attributable to Contractor, Contractor shall pay the City's reasonable costs relating to such audit, including attorney's fees. No review, approval, or audit by the City shall relieve Contractor from liability under this section or under other provisions of this Agreement.
- 53.5. In addition to all other defense and indemnity obligations undertaken by Contractor under this Agreement, Contractor, to the extent that its performance of this Agreement includes the allowance or utilization by members of the public of credit cards to pay monetary obligations to the City or Contractor, or includes the utilization, processing, transmittal and/or storage of credit card data by Contractor, shall defend, release, indemnify and save and hold harmless the City against any and all fines, penalties, assessments, costs, damages or other financial obligations, however denominated, assessed against the City and/or Contractor by credit card company(s), financial institution(s) or by the National Automated Clearing House Association (NACHA) or successor or related entity, including but not limited to, any credit card company fines, regardless of whether considered to be consequential, special, incidental or punitive damages, costs of notifying parties and persons affected by credit card information disclosure, the cost of replacing active credit cards, and any losses associated with fraudulent transaction(s) occurring after a security breach or loss of information with respect to credit card information, and shall defend, release, indemnify, and save and hold harmless the City from any and all claims, demands, suits, actions, liabilities, causes of action or legal or equitable proceedings of any kind or nature, of or by anyone whomsoever, in any way affected by such credit card data or utilizing a credit card in the performance by Contractor of this Agreement. In furtherance of this, Contractor covenants to

defend and indemnify the City and Contractor shall maintain compliance with PCI DSS and with all other requirements and obligations related to credit card data or utilization set out in this Agreement.

ATTACHED EXHIBITS

EXHIBIT A - PARTICIPATING ADDENDUM

EXHIBIT B - CERTIFICATE OF INSURANCE

Contract Control Number: TECHS-202264702-00
Contractor Name: Zivaro, Inc.

IN WITNESS WHEREOF, the parties have set their hands and affixed their seals at Denver, Colorado as of:

SEAL

CITY AND COUNTY OF DENVER:

ATTEST:

By:

APPROVED AS TO FORM:

REGISTERED AND COUNTERSIGNED:

Attorney for the City and County of Denver

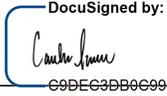
By:

By:

By:

Contract Control Number:
Contractor Name:

TECHS-202264702-00
Zivaro, Inc.

By:  _____
G9DEG3DB0C9945D...

Name: Carolina Palacios
(please print)

Title: Director of Contracts
(please print)

ATTEST: [if required]

By: _____

Name: _____
(please print)

Title: _____
(please print)

**PARTICIPATING ADDENDUM
to NASPO ValuePoint
Cloud Solutions
Administered by the State of Utah
with Zivaro, Inc.
Master Agreement No. AR3102
And
The State of Colorado
Contract # 141379**

1. PARTIES AND SCOPE

This Participating Addendum, including all of its attached exhibits and other documents incorporated by reference (the "Participating Addendum"), is entered into by and between Zivaro, Inc.(the "Contractor"), and the State of Colorado (the "State"). This Participating Addendum covers participation in the **Cloud Solutions** Master Agreement led by the State of Utah (the "Master Agreement"), for use by State agencies and other entities located in Colorado which are authorized by law to utilize State contracts with the prior approval of the State Purchasing Director. The specific Goods and Services provided under the Master Agreement are listed in **Exhibit C Products and Price List** of this agreement.

2. PARTICIPATION

Agencies, political subdivisions and other entities (including cooperatives) authorized by the State's statutes to use State contracts may make purchases under this Participating Addendum as of its Effective Date. Issues of interpretation and eligibility for participation are solely within the authority of the Chief Procurement Officer.

3. STATE MODIFICATIONS TO MASTER AGREEMENT AND APPLICABILITY

To the extent not modified by this Participating Addendum and all its exhibits, the Master Agreement and all its terms and conditions shall apply to this Participating Addendum. If any term of this Participating Addendum conflicts with the Master Agreement, then this Participating Addendum shall control for all transactions between the State and the Contractor under this Participating Addendum. All terms defined in the Master Agreement shall have the meaning given to them in the Master Agreement, except for those terms specifically defined differently in this Participating Addendum.

4. RESERVED

5. PRIMARY CONTACTS AND PERSONNEL RESPONSIBILITIES

The primary contacts for this Participating Addendum are the individuals named in this section. Either Party may change its primary contacts or primary contacts contact information by notice submitted to the other party in writing no later than 5 days following the date on which the change occurs, without a formal amendment to this Participating Addendum. The Contractor's primary

contact shall be ultimately responsible for ensuring that all Goods are delivered and all Services are completed in accordance with this Participating Addendum.

Primary Contact for the State:

Greg Draughon
Colorado State Purchasing & Contracts Office
1525 Sherman Street, 3rd Floor
Denver, CO 80203
303-866-4552
Gregory.Draughon@state.co.us

Primary Contact for the Contractor:

Carolina Palacios
Zivaro, Inc.
990 S. Broadway, Suite 300
Denver, CO 80209
720-836-7387
contracts@zivaro.com

Each individual identified in this §5 of the Participating Addendum shall be the primary contact of the designating Party. All notices required or permitted to be given under this Participating Addendum shall be in writing and shall be delivered (A) by hand with receipt required, (B) by certified or registered mail to such Party's primary contact at the address set forth above or (C) as an email with read receipt requested to the primary contact at the email address, if any, set forth above. If a Party delivers a notice to another through email and the email is undeliverable then, unless the Party has been provided with an alternate email contact, the Party delivering the notice shall deliver the notice by hand with receipt required or by certified or registered mail to such Party's primary contact at the address set forth above. Unless otherwise provided in this Participating Addendum, notices shall be effective upon delivery of the written notice.

In addition to the primary contact in this section, the Contractor shall also provide an individual who is ultimately responsible for the creation and submission of the quarterly volume report described in **Exhibit A** of this Participating Addendum. This individual, as named in this section, shall ensure that all required quarterly volume reports are accurate and delivered by the appropriate due date for that quarterly volume report. The Contractor may change this individual or their contact information by notice submitted to the other party in writing no later than 5 days following the date on which the change occurs, without a formal amendment to this Participating Addendum.

Individual Responsible for Quarterly Volume Report Creation and Submission:

Carolina Palacios
Zivaro, Inc.
990 S. Broadway, Suite 300
Denver, CO 80209
720-836-7387
contracts@zivaro.com

6. SUBCONTRACTORS

The Contractor may only use Subcontractors, as defined in **Exhibit A. §4.DD**, under this Participating Addendum if the State has provided written approval for the Contractor to use that Subcontractor. All such approved Subcontractors authorized in the State of Colorado, as shown on the dedicated Contractor website, are approved to provide sales and service support to the State and any Purchasing Entity in the State. The Contractor's Subcontractor's participation shall be in accordance with the terms and conditions set forth in the Master Agreement and this Participating Addendum, as appropriate.

7. ORDERS

Any Order placed by a Purchasing Entity in the State of Colorado for a Good or Service available under this Participating Addendum shall be deemed to be a sale (and governed by the prices and

other terms and conditions) under the Master Agreement and this Participating Addendum unless the parties to the Order agree in writing that another contract or agreement applies to such Order or the terms of that Order control to the extent that they conflict with the terms of the Master Agreement or this Participating Addendum.

8. ORDER OF PRECEDENCE AND ATTACHED EXHIBITS

All of the exhibits listed in this section are attached to this Participating Addendum and are incorporated herein by reference. In the event of a conflict or inconsistency between this Participating Addendum and any exhibits or attachment such conflict or inconsistency shall be resolved by reference to the documents in the following order of priority:

- A. Colorado Special Provisions in §20 of Exhibit A, State Specific Terms
- B. Exhibit D, Information Technology Specific Terms
- C. The provisions of this Participating Addendum
- D. All other sections of Exhibit A, State Specific Terms
- E. Exhibit B Statement of Work
- F. Exhibit C Products and Price List

Notwithstanding anything to the contrary herein, the State and Purchasing Entities shall not be subject to any provision incorporated in any terms and conditions appearing on Contractor's or Subcontractor's website, any provision incorporated into any click-through or online agreements, or any provisions incorporated into any other document or agreement between the Parties that (i) requires the State to indemnify or hold harmless Contractor or any other party, (ii) is in violation of State law as, regulations, rules, fiscal rules, policies, or other State requirements as deemed solely by the State or (iii) is contrary to any of the provisions incorporated into Exhibit A, §20 or the main body of this Participating Addendum.

THE PARTIES HERETO HAVE EXECUTED THIS AMENDMENT

<p align="center">CONTRACTOR Zivaro, Inc.</p> <p>By: <u>Todd E. Olson</u> Title: <u>VP Sales - SHED</u></p> <p>By: <u>[Signature]</u> *Signature</p> <p>Date: <u>9-3-2019</u></p>	<p align="center">STATE OF COLORADO Jared S. Polis, Governor</p> <p align="center">Department of Personnel & Administration State Purchasing and Contracts Office Kara Veitch, Executive Director</p> <p>By: <u>[Signature]</u> Cindy Lombardi, State Purchasing and Contracts Director</p> <p>Date: <u>9/30/19</u></p>
--	--

STATE OF COLORADO
Governor's Office of Information Technology
Theresa M. Szcurek PhD., Information Officer and Executive Director

By: [Signature]
_____, Deputy Secretary of Technology and
Chief Financial Officer

Date: 10/17/19

ALL CONTRACTS REQUIRE APPROVAL BY THE STATE CONTROLLER

§24-30-202 C.R.S. requires the State Controller to approve all State Contracts. This Participating Addendum is not valid until signed and dated below by the State Controller or an authorized delegate.

STATE CONTROLLER
Robert Jaros, CPA, MBA, JD

By: [Signature]

Name: JOSEPH WEBER, Delegate

Date: 10-24-19

**PARTICIPATING ADDENDUM
EXHIBIT A
STATE SPECIFIC TERMS**

1.	AUTHORITY	5
2.	PURPOSE.....	5
3.	TERM	5
4.	DEFINITIONS	6
5.	STATEMENT OF WORK	10
6.	PAYMENTS TO CONTRACTOR	10
7.	PAYMENTS TO STATE.....	12
8.	REPORTING – NOTIFICATION.....	12
9.	CONTRACTOR RECORDS.....	14
10.	CONFIDENTIAL INFORMATION-STATE RECORDS.....	15
11.	CONFLICTS OF INTEREST.....	16
12.	INSURANCE	17
13.	BREACH OF CONTRACT	19
14.	REMEDIES	19
15.	DISPUTE RESOLUTION.....	21
16.	RIGHTS IN WORK PRODUCT AND OTHER INFORMATION.....	22
17.	OBLIGATIONS AND RIGHTS IN THE EVENT OF TERMINATION OF ORDER OR CONTRACT.....	23
18.	STATEWIDE CONTRACT MANAGEMENT SYSTEM	24
19.	GENERAL PROVISIONS	24
20.	COLORADO SPECIAL PROVISIONS (COLORADO FISCAL RULE 3-3).....	27
	EXHIBIT B STATEMENT OF WORK.....	B
	EXHIBIT C PRODUCTS AND PRICE LIST	C
	PARTICIPATING ADDENDUM EXHIBIT D, INFORMATION TECHNOLOGY PROVISIONS.....	D

1. AUTHORITY

Authority to enter into this Participating Addendum exists in the Colorado Procurement Code, §24-102-202, C.R.S. and 1 CCR 101-9 R-24-102-202-01., and its associated rules.

2. PURPOSE

The Parties are entering into this Participating Addendum for the Contractor to provide **Cloud Services** to Purchasing Entities. The Contractor was selected as a result of State Price Agreement.

3. TERM

A. Initial Term - Work Commencement

The Parties' respective performances under this Participating Addendum shall commence on the Effective Date and shall be co-terminus with NASPO ValuePoint Master Agreement AR2472. Unless this Participating Addendum is terminated earlier, as described herein, or the State cancels its participation as described in the Master Agreement (the "Term"), the term of the Participating Addendum shall follow the Master Agreement initial term and will

be automatically extended beyond the initial term if the Master Agreement term is extended (See Section 3.B.).

B. Extension of Term

If the term of NASPO ValuePoint Master Agreement is extended for any reason, the Term of this Participating Addendum shall be automatically modified to account for that extension, so long as such extension complies with the Colorado Procurement Code.

C. Order Term

Orders may only be placed prior to the expiration or earlier termination of this Participating Addendum, but may have a delivery date or performance period that extends no longer than 120 calendar days following that expiration or earlier termination date. Regardless of whether this Participating Addendum has expired or has been terminated, the Contractor shall comply with all Orders that extend past the expiration or termination, as described in this section, and all requirements of this Participating Addendum necessary to complete outstanding Orders shall survive the expiration or termination of this Participating Addendum until all Orders are complete.

D. Early Termination in the Public Interest

The State is entering into this Participating Addendum to serve the public interest of the State of Colorado as determined by its Governor, General Assembly, or Courts. A determination that this Contract should be terminated in the public interest shall not be equivalent to a State right to terminate for convenience. This subsection shall not apply to a termination of this Participating Addendum by the State for breach by Contractor, which shall be governed by §14.A.i.

i. Method and Content

The State shall notify Contractor of such termination in accordance with §5 of this Participating Addendum. The notice shall specify the effective date of the termination and whether it affects all or a portion of this Participating Addendum, and shall include, to the extent practicable, the public interest justification for the termination.

ii. Obligations and Rights

Upon receipt of notice for termination in the public interest, Contractor shall be subject to the rights and obligations set forth in §14.A.i.a

iii. Payments

If the State terminates this Participating Addendum in the public interest, the Purchasing Entities shall pay Contractor according to their orders with the Contractor. The sum of any and all payments shall not exceed the maximum amount payable to Contractor under each order.

4. DEFINITIONS

The following terms shall be construed and interpreted as follows:

- A. "Administration Fee"** means the fee that is due to the State for the administration of this Participating Addendum, as described in §7. A. of this **Exhibit A**.

- B. **“Breach of Contract”** means the failure of a Party to perform any of its obligations in accordance with this Contract, in whole or in part or in a timely or satisfactory manner. The institution of proceedings under any bankruptcy, insolvency, reorganization or similar law, by or against Contractor, or the appointment of a receiver or similar officer for Contractor or any of its property, which is not vacated or fully stayed within thirty (30) days after the institution of such proceeding, shall also constitute a breach. If Contractor is debarred or suspended under §24-109-105, C.R.S. at any time during the term of this Contract, then such debarment or suspension shall constitute a breach.
- C. **“Business Day”** means any day in which the State is open and conducting business, but shall not include Saturday, Sunday or any day on which the State observes one of the holidays listed in §24-11-101(1), C.R.S.
- D. **“Ceiling Price”** means the maximum price a Contractor or a Subcontractor may charge for a Good or Service under this Participating Addendum.
- E. **“Chief Procurement Officer”** means the individual to whom the Executive Director of the Department of Personnel & Administration has delegated his or her authority pursuant to §24-102-202, C.R.S. to procure or supervise the procurement of all supplies and services needed by the state.
- F. **“CJI”** means criminal justice information collected by criminal justice agencies needed for the performance of their authorized functions, including, without limitation, all information defined as criminal justice information by the U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Security Policy, as amended, and all Criminal Justice Records as defined under §24-72-302, C.R.S.
- G. **“Confidential Information”** means any and all information that is normally considered confidential in nature, and includes, but is not limited to, all State Records not subject to disclosure under the Colorado Open Records Act, §§24-72-200.1, *et seq.*, C.R.S. (“CORA”).
- H. **“Contract”** means this Participating Addendum, including all attached Exhibits, all documents incorporated by reference, all referenced statutes, rules and cited authorities, and any future modifications thereto.
- I. **“Contract Funds”** means the funds that have been appropriated, designated, encumbered, or otherwise made available for payment by a Purchasing Entity for Orders placed under this Participating Addendum.
- J. **“CORA”** means the Colorado Open Records Act, §§24-72-200.1, *et seq.*, C.R.S.
- K. **“Deliverable”** means the outcome to be achieved or output to be provided, in the form of a tangible object or software that is produced as a result of Contractor’s Work that is intended to be delivered to the State by Contractor.
- L. **“Effective Date”** means the date Contract is signed by the State Controller or their designee.
- M. **“Environmentally Preferable Products”** means products that have a lesser or reduced adverse effect on human health and the environment when compared with competing products that serve the same purpose, as defined in §24-103-904, C.R.S.
- N. **“Effective Date”** means the date on which this Participating Addendum is approved and signed by the Colorado State Controller or designee, as shown on the Signature Page for this Participating Addendum. If this Contract is for a Major Information Technology Project, as defined in §24-37.5-102(2.6), C.R.S., then the Effective Date of this Contract shall be the

later of the date on which this Contract is approved and signed by the State's Chief Information Officer or authorized delegate or the date on which this Contract is approved and signed by the State Controller or authorized delegate, as shown on the Signature Page for this Contract.

- O. **"Exhibits"** means the following exhibits attached to this Contract:
- i. **Exhibit A**, State Specific Terms.
 - ii. **Exhibit B**, Statement of Work.
 - iii. **Exhibit C**, Products and Price List
 - iv. **Exhibit D**, OIT terms and conditions
- P. **"Extension Term"** means the time period defined in §3. B.
- Q. **"Goods"** means any movable material acquired, produced, or delivered by Contractor as set forth in this Participating Addendum and shall include any movable material acquired, produced, or delivered by Contractor in connection with the Services.
- R. **"Incident"** means any accidental or deliberate event that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of any communications or information resources of the State, which are included as part of the Work, as described in §§24-37.5-401, *et. seq.*, C.R.S. Incidents include, without limitation (i) successful attempts to gain unauthorized access to a State system or State Information regardless of where such information is located; (ii) unwanted disruption or denial of service; (iii) the unauthorized use of a State system for the processing or storage of data; or (iv) changes to State system hardware, firmware, or software characteristics without the State's knowledge, instruction, or consent.
- S. **"Initial Term"** means the time period defined in §3.A of this **Exhibit A**.
- T. **"Order"** means any delivery order, purchase order, contract, agreement or other binding document used by a Purchasing Entity to order the Goods and Services described in this Participating Addendum from the Contractor, and shall include any modification to such a document.
- U. **"Party"** means the State or Contractor, and **"Parties"** means both the State and Contractor.
- V. **"Purchasing Entity"** means any entity or organization that has been authorized by the State to place Orders with the Contractor, and may include, without limitation, agencies of the State, government supported institution of higher education within the State, political subdivisions of the State, authorized non-profit organizations and other authorized entities.
- W. **"PCI"** means payment card information including any data related to credit card holders' names, credit card numbers, or the other credit card information as may be protected by state or federal law.
- X. **"PII"** means personally identifiable information including, without limitation, any information maintained by the State about an individual that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. PII includes, but is not limited to, all information defined as personally identifiable information in §§24-72-501 and 24-73-101, C.R.S.

- Y. **“PHI”** means any protected health information, including, without limitation any information whether oral or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. PHI includes, but is not limited to, any information defined as Individually Identifiable Health Information by the federal Health Insurance Portability and Accountability Act.
- Z. **“Services”** means the services to be performed by Contractor as set forth in this Participating Addendum, and shall include any services to be rendered by Contractor in connection with the Goods.
- AA. **“State Confidential Information”** means any and all State Records not subject to disclosure under CORA. State Confidential Information shall include, but is not limited to, PII, PCI, and State personnel records not subject to disclosure under CORA. State Confidential Information shall not include information or data concerning individuals that is not deemed confidential but nevertheless belongs to the State, which has been communicated, furnished, or disclosed by the State to Contractor which (i) is subject to disclosure pursuant to CORA; (ii) is already known to Contractor without restrictions at the time of its disclosure to Contractor; (iii) is or subsequently becomes publicly available without breach of any obligation owed by Contractor to the State; (iv) is disclosed to Contractor, without confidentiality obligations, by a third party who has the right to disclose such information; or (v) was independently developed without reliance on any State Confidential Information.
- BB. **“State Fiscal Rules”** means that fiscal rules promulgated by the Colorado State Controller pursuant to §24-30-202(13) (a), C.R.S.
- CC. **“State Fiscal Year”** means a 12-month period beginning on July 1 of each calendar year and ending on June 30 of the following calendar year. If a single calendar year follows the term, then it means the State Fiscal Year ending in that calendar year.
- DD. **“State Records”** means any and all State data, information, and records, regardless of physical form, including, but not limited to, information subject to disclosure under CORA.
- EE. **“Subcontractor”** means third-parties, if any, engaged by Contractor pursuant to §19.B. to aid in performance of the Work. The term “Subcontractor” includes, without limitation, any dealers, distributors, partners or resellers engaged by the Contractor to perform the Work.
- FF. **“Tax Information”** means federal and State of Colorado tax information including, without limitation, federal and State tax returns, return information, and such other tax-related information as may be protected by federal and State law and regulation. Tax Information includes, but is not limited to all information defined as federal tax information in Internal Revenue Service Publication 1075.
- GG. **“Work”** means the Goods delivered and Services performed pursuant to this Contract.
- HH. **“Work Product”** means the tangible and intangible results of the Work, whether finished or unfinished, including drafts. Work Product includes, but is not limited to, documents, text, software (including source code), research, reports, proposals, specifications, plans, notes, studies, data, images, photographs, negatives, pictures, drawings, designs, models, surveys, maps, materials, ideas, concepts, know-how, and any other results of the Work. “Work Product” does not include any material that was developed prior to the Effective Date that is used, without modification, in the performance of the Work.

Any other term used in this Participating Addendum that is defined in an Exhibit shall be construed and interpreted as defined in that Exhibit.

5. STATEMENT OF WORK

Contractor shall complete the Work as described in this Participating Addendum and in accordance with the provisions of Exhibits A, B, and C and with any Purchasing Entity's Order. Contractor personnel shall work cooperatively with State and Purchasing Entity staff to ensure the completion of the Work.

A. Ordering and Order Fulfillment

i. Ordering

- a. Contractor shall provide a complete and accurate Internal Revenue Service form W9 to the State prior to accepting an Order from any Purchasing Entity. Upon a request by a Purchasing Entity, Contractor shall provide a complete and accurate Internal Revenue Service form W9 to that Purchasing Entity.
- b. Each Purchasing Entity may complete an Order in accordance with its own rules and policies, as available to Contractor, using the appropriate documentation for that organization to issue an Order.
- c. Contractor shall communicate directly with each Purchasing Entity related to that Purchasing Entity's Orders.
- d. Contractor shall ensure that all Orders it accepts have the proper information contained in them for Contractor to be able to comply with all reporting requirements of this Exhibit A.
- e. If Contractor provides for Ordering through an internet-based portal or electronic catalog, Contractor shall maintain all of Contractor's necessary hardware, software, backup-capacity and network connections required to operate that internet-based portal or electronic catalog.
- f. Contractor's internet-based portal and electronic catalogs shall clearly designate that they are part of this Participating Addendum and shall have a link to the State's price agreement web location, as determined by the State. Contractor shall ensure that all Environmentally Preferable Products are clearly listed on internet-based portal and electronic catalogs.
- g. If Contractor provides an internet-based portal or electronic catalog, Contractor shall also provide paper catalogs or catalogs on other digital media upon request by a Purchasing Entity.
- h. If Contractor's catalog will be either hosted on or accessed through the State's eCommerce system, when available, then Contractor shall comply with all policies, procedures and directions from the State in relation to hosting its catalog on or making its catalog accessible through that system. Contractor shall ensure that all information made available through the State's eCommerce system is accurate and complies with this Participating Addendum.

6. PAYMENTS TO CONTRACTOR

A. Payments Under Orders

- i. Contractor shall allow the State and Purchasing Entities to use a procurement card or other credit card to make payments under any Order, in addition to any other payment procedure available to the State or Purchasing Entity.
- ii. The State shall not pay any amount to Contractor under this Participating Addendum unless the State issues an Order, at which time it shall pay Contractor in accordance with that Order. The State shall not be responsible for payment under any Order that is issued by a Purchasing Entity that is not the State, and the Contractor shall seek no payment or other compensation from the State for any Work performed under any Order issued by a Purchasing Entity that is not the State.

B. Payment Procedures

i. Invoices

Contractor shall invoice each Purchasing Entity in accordance with that Purchasing Entity's Order. Contractor shall not invoice the State under any Order unless the State issued that Order. Contractor shall allow 45 days for the State and Purchasing Entities to pay an invoice following the receipt of the invoice, unless the State or a Purchasing Entity specifically agrees to a shorter time in an Order. State law and regulations provide that State payments made within 45 days are not considered delinquent, and unless otherwise agreed, State Purchasing Entities will pay interest on any unpaid balance beginning on the 45th day at the rate of 1% per month until paid in full; provided, however, that interest shall not accrue on unpaid amounts that are the subject of a good faith dispute regarding the obligation to pay all or a portion of the liability. Contractor shall invoice State Ordering Entities separately for accrued interest on delinquent amounts due. The billing shall reference the delinquent payment, the number of day's interest to be paid, and the applicable interest rate. (§ 24-30-202(24), C.R.S., as amended.)

ii. Payment Disputes

Unless different procedures are specified in an Order, if Contractor disputes any calculation, determination or amount of any payment, Contractor shall notify the Purchasing Entity issuing the Order in writing of its dispute within 30 days following the earlier to occur of Contractor's receipt of the payment or notification of the determination or calculation of the payment by that Purchasing Entity. The Purchasing Entity will review the information presented by Contractor and may make changes to its determination based on this review. The calculation, determination or payment amount that results from the Purchasing Entity's review shall not be subject to additional dispute under this subsection. No payment subject to a dispute under this subsection shall be due until after the Purchasing Entity has concluded its review, and the Purchasing Entity shall not pay any interest on any amount during the period it is subject to dispute under this subsection.

iii. Available Funds-Contingency-Termination of Order

Purchasing Entities, except for authorized non-profit entities, are prohibited by law from making commitments beyond the term of the current Purchasing Entity's Fiscal Year. Payment to Contractor beyond the current Purchasing Entity's Fiscal Year is contingent on the appropriation and continuing availability of Contract Funds in any subsequent year (See Colorado Special Provision). If federal funds, non-State funds or funds from any other source constitute all or some of the Contract Funds, the Purchasing

Entity's obligation to pay Contractor shall be contingent upon such funding continuing to be made available for payment. Orders under this Participating Addendum shall be made only from Contract Funds, and the Purchasing Entity's liability for such payments shall be limited to the amount remaining of such Contract Funds. If State, federal or other Purchasing Entity funds are not appropriated, or otherwise become unavailable to fund an Order under this Participating Addendum, the Purchasing Entity may, upon written notice, terminate the Order, in whole or in part, without incurring further liability. The Purchasing Entity shall, however, remain obligated to pay for Services and Goods that are delivered and accepted prior to the effective date of notice of termination of Order. A State Purchasing Entity Order termination shall otherwise be treated as if the Order was terminated in the public interest as described in §3. D. of this Exhibit A.

The Purchasing Entity may effect such termination by giving Contractor a written notice of termination, to the Contractor's primary contact in accordance with §5 of the Participating Addendum, and by paying to Contractor any amounts which are due and have not been paid through the last day of the Fiscal Year for which appropriated funds are available. The Purchasing Entity shall endeavor to give notice of such termination not less than 30 days prior to the day of non-availability of funds, and shall notify Contractor of any anticipated termination.

iv. **Discount and Delinquency Period**

Any applicable cash discount period or delinquency period for the amounts shown on an invoice shall begin on the date the Purchasing Entity's approves of the invoice, or from the date of receipt of acceptable Goods or Services at the specified destination by an authorized Purchasing Entity representative, whichever is later.

7. PAYMENTS TO STATE

Administrative Fees

- A. Each State Fiscal Year quarter, Contractor shall, using a form as directed by the State, calculate an Administrative Fee equal to 1% of the total sales made under Orders during that State Fiscal Year quarter. Contractor shall pay the State the Administrative Fee for each State Fiscal Year quarter within 45 days following the end of that State Fiscal Year quarter.
- B. Contractor shall remit all administrative fees to the State's primary contact identified in §5 of the Participating Addendum and with the payee as "State of Colorado".

8. REPORTING – NOTIFICATION

A. Volume Reporting

The State will use a centralized method of tracking volume. Contractor shall provide a quarterly volume report to the State's primary contact identified in §5 of this Participating Addendum within 30 calendar days following the end of the State Fiscal Year quarter that the report covers. The quarterly volume report shall be submitted in a form as directed by the State, which may be modified by the State from time to time. The quarterly volume report shall contain, at a minimum, all of the following:

- i. A summary volume report that includes, but is not limited to, all of the following for the quarter that the report covers:
 - a. The total spent by each type of Purchasing Entity under this Participating

Addendum.

- b. The total of the list cost of all items purchased by each type of Purchasing Entity under this Participating Addendum.
 - c. The total estimated cost savings for each type of Purchasing Entity under this Participating Addendum, calculated as the total list cost of all items purchased by each type of Purchasing Entity minus the total spent for that type of Purchasing Entity.
 - d. The total paid with a procurement card or credit card for each Purchasing Entity under this Participating Addendum.
 - e. The total sales of environmentally preferable products, as defined in the State's Environmentally Preferable Purchasing Policy, for each Purchasing Entity under this Participating Addendum.
 - f. The amount of the total administrative fee due to the State.
 - g. Any additional summary information as requested by the State.
- ii. A detail report that includes, but is not limited to, all of the following for each sale that occurred during the quarter that the report covers:
- a. The name of the Purchasing Entity who the sale was made to.
 - b. The date of the sale.
 - c. A listing of each item purchased in the sale, including the name of the item, the quantity of the item, the unit price for the item, the extended cost for the item calculated by multiplying the unit price by the quantity, the list price per unit for the item, the extended list cost for the item calculated by multiplying the quantity by the list price, and the savings on the item calculated by subtracting the extended cost from the extended list cost.
 - d. Any other detail information as requested by the State.

B. Additional Operational Reporting

Upon request by the State, the Contractor shall provide operational reporting that include all detailed and summary transaction, historical or payment information related to the State or any of the Participating Entities as requested by the State. The Contractor shall provide all such additional reports within 10 Business Days following the State's request for that information, unless the State agrees to a longer period of time in writing.

C. Environmentally Preferable Product Reporting

Upon request by the State, the Contractor shall provide detailed reporting on environmentally preferable products, as defined in the State's Environmentally Preferable Purchasing Policy that are purchased or made available under this Participating Addendum. The State and the Contractor shall agree upon the scope and detail of such reports. The Contractor shall provide all such additional reports within 10 Business Days following the State's request for that information, unless the State agrees to a longer period of time in writing.

D. Litigation Reporting

If Contractor is served with a pleading or other document in connection with an action before a court or other administrative decision making body, and such pleading or document relates

to this Participating Addendum or may affect Contractor's ability to perform its obligations under this Participating Addendum, Contractor shall, within 10 days after being served, notify the State of such action and deliver copies of such pleading or document to the State's primary contact identified in §5 of the Participating Addendum .

E. Performance Outside the State of Colorado or the United States, §24-102-206, C.R.S.

To the extent not previously disclosed in accordance with §24-102-206, C.R.S., Contractor shall provide written notice to the State's primary contact in accordance with §5 of the Participating Addendum and in a form designated by the State, within 20 days following the earlier to occur of Contractor's decision to perform Services outside of the State of Colorado or the United States, or its execution of an agreement with a Subcontractor to perform Services outside the State of Colorado or the United States. Such notice shall specify the type of Services to be performed outside the State of Colorado or the United States and the reason why it is necessary or advantageous to perform such Services at such location or locations, and such notice shall be a public record. Knowing failure by Contractor to provide notice to the State under this section shall constitute a breach of this Participating Addendum. This section shall not apply if the Participating Addendum Funds include any federal funds.

9. CONTRACTOR RECORDS

A. Maintenance

Contractor shall maintain a file of all documents, records, communications, notes and other materials relating to the Work (the "Contractor Records") performed by the Contractor and any Subcontractors, that are required to ensure proper performance of that Work. Contractor shall maintain Contractor Records until the last to occur of: (i) the date three years after the date this Participating Addendum expires or is terminated, (ii) final payment under this Participating Addendum is made, (iii) the resolution of any pending Contract matters, or (iv) if an audit is occurring, or Contractor has received notice that an audit is pending, the date such audit is completed and its findings have been resolved (the "Record Retention Period").

B. Inspection

Contractor shall permit the State to audit, inspect, examine, excerpt, copy and transcribe Contractor Records during the Record Retention Period. Contractor shall make Contractor Records available during normal business hours at Contractor's office or place of business, or at other mutually agreed upon times or locations, upon no fewer than two Business Days' notice from the State, unless the State determines that a shorter period of notice, or no notice, is necessary to protect the interests of the State.

C. Monitoring

The State, in its discretion, may monitor Contractor's performance of its obligations under this Participating Addendum using procedures as determined by the State. The State shall monitor Contractor's performance in a manner that does not unduly interfere with Contractor's performance of the Work.

D. Final Audit Report

Contractor shall promptly submit to the State a copy of any final audit report of an audit performed on Contractor's records that relates to or affects this Participating Addendum or the Work, whether the audit is conducted by Contractor or a third party.

E. Periodic Business Reviews

- i. The State may schedule periodic business reviews to review Contractor's performance under this Participating Addendum.
- ii. Contractor shall ensure personnel assigned to the Participating Addendum are available for these meetings with the State as scheduled by the State.
- iii. Contractor's primary contact designated in §5 of this the Participating Addendum shall be available for all regularly scheduled meetings between Contractor and the State, unless the State has granted prior, written approval otherwise.

10. CONFIDENTIAL INFORMATION-STATE RECORDS

A. Confidentiality

Contractor shall keep confidential, and cause all Subcontractors to keep confidential, all State Records, unless those State Records are publicly available. Contractor shall not, without prior written approval of the State, use, publish, copy, disclose to any third party, or permit the use by any third party of any State Records, except as otherwise stated in this Participating Addendum, permitted by law or approved in Writing by the State. Contractor shall provide for the security of all State Confidential Information in accordance with all policies promulgated by the Colorado Office of Information Security and all applicable laws, rules, policies, publications, and guidelines. If Contractor or any of its Subcontractors will or may receive the following types of data, Contractor or its Subcontractors shall provide for the security of such data according to the following: (i) the most recently promulgated IRS Publication 1075 for all Tax Information and in accordance with the Safeguarding Requirements for Federal Tax Information attached to this Contract as an Exhibit, if applicable, (ii) the most recently updated PCI Data Security Standard from the PCI Security Standards Council for all PCI, (iii) the most recently issued version of the U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Security Policy for all CJI, and (iv) the federal Health Insurance Portability and Accountability Act for all PHI and the HIPAA Business Associate Agreement attached to this Contract , if applicable.. Contractor shall immediately forward any request or demand for State Records to the State's primary contact as identified in §5 of the Participating Addendum.

B. Other Entity Access and Nondisclosure Agreements

Contractor may provide State Records to its agents, employees, assigns and Subcontractors as necessary to perform the Work, but shall restrict access to State Confidential Information to those agents, employees, assigns and Subcontractors who require access to perform their obligations under this Participating Addendum. Contractor shall ensure all such agents, employees, assigns, and Subcontractors sign agreements containing nondisclosure provisions at least as protective as those in this Participating Addendum, and that the nondisclosure provisions are in force at all times the agent, employee, assign or Subcontractor has access to any State Confidential Information. Contractor shall provide copies of those signed nondisclosure provisions to the State upon execution of the nondisclosure provisions.

C. Use, Security, and Retention

Contractor shall use, hold and maintain State Confidential Information in compliance with all applicable laws and regulations in facilities located within the United States, and shall maintain a secure environment that ensures confidentiality of all State Confidential Information wherever located. Contractor shall provide the State with access, subject to Contractor's reasonable security requirements, for purposes of inspecting and monitoring access and use of State Confidential Information and evaluating security control

effectiveness. Upon the expiration or termination of this Participating Addendum, Contractor shall return State Records provided to Contractor or destroy such State Records and certify to the State that it has done so, as directed by the State. If Contractor is prevented by law or regulation from returning or destroying State Confidential Information, Contractor warrants it will guarantee the confidentiality of, and cease to use, such State Confidential Information.

D. Incident Notice and Remediation

If Contractor becomes aware of any Incident, it shall notify the State immediately and cooperate with the State regarding recovery, remediation, and the necessity to involve law enforcement, as determined by the State. Unless Contractor can establish that neither Contractor nor any of Contractor's agents, employees, assigns or Subcontractors are the cause or source of the Incident, Contractor shall be responsible for the cost of notifying each person who may have been impacted by the Incident. After an Incident, Contractor shall take steps to reduce the risk of incurring a similar type of Incident in the future as directed by the State, which may include, but is not limited to, developing and implementing a remediation plan that is approved by the State at no additional cost to the State. The State may adjust or direct modifications to this plan in its sole discretion, and Contractor shall make all modifications as directed by the State. If Contractor cannot produce its analysis and plan within the allotted time, the State, in its sole discretion, may perform such analysis and produce a remediation plan, and Contractor shall reimburse the State for the actual costs thereof. The State may, in its sole discretion and at Contractor's sole expense, require Contractor to engage the services of an independent, qualified, State-approved third party to conduct a security audit. Contractor shall provide the State with the results of such audit and evidence of Contractor's planned remediation in response to any negative findings.

E. Data Protection and Handling

Contractor shall ensure that all State Records and Work Product in the possession of Contractor or any Subcontractors are protected and handled in accordance with the requirements of this Contract, including the requirements of any Exhibits hereto, at all times.

F. Safeguarding PII

If Contractor or any of its Subcontractors will or may receive PII under this Contract, Contractor shall provide for the security of such PII, in a manner and form acceptable to the State, including, without limitation, State non-disclosure requirements, use of appropriate technology, security practices, computer access security, data access security, data storage encryption, data transmission encryption, security inspections, and audits. Contractor shall be a "Third-Party Service Provider" as defined in §24-73-103(1) (i), C.R.S. and shall maintain security procedures and practices consistent with §§24-73-101 *et seq.*, C.R.S.

11. CONFLICTS OF INTEREST

A. Actual Conflicts of Interest

Contractor shall not engage in any business or activities, or maintain any relationships that conflict in any way with the full performance of the obligations of Contractor under this Participating Addendum. Such a conflict of interest would arise when a Contractor or Subcontractor's employee, officer or agent were to offer or provide any tangible personal benefit to an employee of the State, or any member of his or her immediate family or his or her partner, related to the award of, entry into or management or oversight of this Participating Addendum.

B. Apparent Conflicts of Interest

Contractor acknowledges that, with respect to this Participating Addendum, even the appearance of a conflict of interest shall be harmful to the State's interests. Absent the State's prior written approval, Contractor shall refrain from any practices, activities or relationships that reasonably appear to be in conflict with the full performance of Contractor's obligations under this Participating Addendum.

C. Disclosure to the State

If a conflict or the appearance of a conflict arises, or if Contractor is uncertain whether a conflict or the appearance of a conflict has arisen, Contractor shall submit to the State a disclosure statement setting forth the relevant details for the State's consideration. Failure to promptly submit a disclosure statement or to follow the State's direction about the actual or apparent conflict constitutes a breach of this Participating Addendum.

12. INSURANCE

Contractor shall obtain and maintain, and ensure that each Subcontractor shall obtain and maintain, insurance as specified in this section at all times during the term of this Participating Addendum and until all orders for goods or Services or both have been delivered and accepted, regardless of whether this Participating Addendum has expired or has been terminated. All insurance policies required by this Participating Addendum shall be issued by insurance companies as approved by the State.

A. Workers' Compensation

Workers' Compensation insurance as required by state statute, and employers' liability insurance covering all Contractor or Subcontractor employees acting within the course and scope of their employment. Insurance must stay in place and in effect even if the contract terms expires, until all product or terms of the contract are completed and satisfied up to 120 days after contract term expires.

B. General Liability

Commercial general liability insurance covering premises operations, fire damage, independent contractors, products and completed operations, blanket contractual liability, personal injury, and advertising liability with minimum limits as follows:

- i. \$1,000,000 each occurrence;
- ii. \$2,000,000 general aggregate;
- iii. \$1,000,000 products and completed operations aggregate; and
- iv. \$50,000 any one fire.

C. Automobile Liability

Automobile liability insurance covering any auto (including owned, hired and non-owned autos) with a minimum limit of \$1,000,000 each accident combined single limit.

D. Cyber/ Network Security and Privacy Liability

Cyber/ Network Security and Privacy Liability Insurance in an amount of not less than \$3,000,000 combined single limit to cover civil, regulatory and statutory damages, contractual damage, as well as data breach management exposure, and any loss of income or extra expense as a result of actual or alleged breach, violation or infringement of right to

privacy, consumer data protection law, confidentiality or other legal protection for personal information, as well as confidential information of Company or Company Clients.

E. Professional Liability Insurance

Professional liability and errors and omissions coverage for claims for damages resulting from or arising out of any professional services provided by the Vendor in an amount of not less than \$3,000,000.00 per claim and aggregate.

The above requirements for Cyber/Network Security and Privacy Liability and Professional Errors & Omissions can be met by separate policies or a combination of these coverages under one policy form with minimum limits \$5,000,000 each occurrence and in the aggregate.

F. Crime Insurance

Crime insurance including employee dishonesty coverage with minimum limits as follows:

- i. \$1,000,000 each occurrence; and
- ii. \$1,000,000 general aggregate.

G. Additional Insured

The State shall be named as additional insured on all commercial general liability policies (leases and construction contracts require additional insured coverage for completed operations) required of Contractor and Subcontractors.

H. Primacy of Coverage

Coverage required of Contractor and each Subcontractor shall be primary over any insurance or self-insurance program carried by Contractor or the State.

I. Cancellation

The above insurance policies shall include provisions preventing cancellation or non-renewal, except for cancellation based on non-payment of premiums, without at least 30 days prior notice to Contractor and Contractor shall forward such notice to the State in accordance with §5 of the Participating Addendum within 7 days of Contractor's receipt of such notice.

J. Subrogation Waiver

All insurance policies secured or maintained by Contractor or its Subcontractors in relation to this Participating Addendum shall include clauses stating that each carrier shall waive all rights of recovery under subrogation or otherwise against Contractor or the State, its agencies, institutions, organizations, officers, agents, employees, and volunteers.

K. Public Entities

If Contractor is a "public entity" within the meaning of the Colorado Governmental Immunity Act, §§24-10-101, *et seq.*, C.R.S. (the "GIA"), Contractor shall maintain, in lieu of the liability insurance requirements stated above, at all times during the term of this Participating Addendum such liability insurance, by commercial policy or self-insurance, as is necessary to meet its liabilities under the GIA. If a Subcontractor is a public entity within the meaning of the GIA, Contractor shall ensure that the Subcontractor maintain at all times during the terms of this Participating Addendum, in lieu of the liability insurance requirements stated above, such liability insurance, by commercial policy or self-insurance, as is necessary to meet the Subcontractor's obligations under the GIA.

L. Certificates

Contractor shall provide to the State certificates evidencing Contractor's insurance coverage required in this Participating Addendum within seven Business Days following the Effective Date. Contractor shall provide to the State certificates evidencing Subcontractor insurance coverage required under this Participating Addendum within seven Business Days following the Effective Date, except that, if Contractor's subcontract is not in effect as of the Effective Date, Contractor shall provide to the State certificates showing Subcontractor insurance coverage required under this Participating Addendum within seven Business Days following Contractor's execution of the subcontract. No later than 15 days before the expiration date of Contractor's or any Subcontractor's coverage, Contractor shall deliver to the State certificates of insurance evidencing renewals of coverage. At any other time during the term of this Participating Addendum, upon request by the State, Contractor shall, within seven Business Days following the request by the State, supply to the State evidence satisfactory to the State of compliance with the provisions of this §12.

13. BREACH OF CONTRACT

In the event of a Breach of Contract, the aggrieved Party shall give written notice of breach to the other Party. If the notified Party does not cure the Breach of Contract, at its sole expense, within 30 days after the delivery of written notice, the Party may exercise any of the remedies as described in §14 for that Party. Notwithstanding any provision of this Participating Addendum to the contrary, the State, in its discretion in order to protect the public interest of the State, need not provide notice or a cure period and may immediately terminate this Participating Addendum in whole or in part or institute any other remedy in this Participating Addendum; or if Contractor is debarred or suspended under §24-109-105, C.R.S., the State, in its discretion, need not provide notice or cure period and may terminate this Contract in whole or in part or institute any other remedy in this Contract as of the date that the debarment or suspension takes effect.

14. REMEDIES

A. State's Remedies

If Contractor is in breach under any provision of this Participating Addendum and fails to cure such breach, the State, following the notice and cure period set forth in §13, shall have all of the remedies listed in this section in addition to all other remedies set forth in this Participating Addendum or at law. The State may exercise any or all of the remedies available to it, in its discretion, concurrently or consecutively.

i. Termination for Breach

In the event of Contractor's uncured breach, the State may terminate this entire Participating Addendum or any part of this Participating Addendum. Contractor shall continue performance of this Participating Addendum to the extent not terminated, if any.

If after termination by the State, the State agrees that Contractor was not in breach or that Contractor's action or inaction was excusable, such termination shall be treated as a termination in the public interest, and the rights and obligations of the Parties shall be as if this Participating Addendum had been terminated in the public interest under §3.

D.

ii. Remedies Not Involving Termination

The State, in its discretion, may exercise one or more of the following additional remedies:

a. Suspend Performance

Suspend Contractor's performance with respect to all or any portion of the Work pending corrective action as specified by the State without entitling Contractor to an adjustment in price or cost or an adjustment in the performance schedule. Contractor shall promptly cease performing Work and incurring costs in accordance with the State's directive, and neither the State nor any Purchasing Entity shall be liable for costs incurred by Contractor after the suspension of performance.

b. Removal

Demand immediate removal of any of Contractor's employees, agents, or Subcontractors from the Work whom the State deems incompetent, careless, insubordinate, unsuitable, or otherwise unacceptable or whose continued relation to this Participating Addendum is deemed by the State to be contrary to the public interest or the State's best interest.

c. Intellectual Property

If any Work infringes, or if the State in its sole discretion determines that any Work is likely to infringe, a patent, copyright, trademark, trade secret or other intellectual property right, Contractor shall, at the option of and as approved by the State or Purchasing Entity (i) secure that right to use such Work for the State, Purchasing Entity and Contractor; (ii) replace the Work with noninfringing Work or modify the Work so that it becomes noninfringing; or, (iii) remove any infringing Work and refund the amount paid for such Work to the Purchasing Entity.

B. Contractor's Remedies

If the State is in breach of any provision of this Participating Addendum and does not cure such breach, Contractor, following the notice and cure period in §13 and the dispute resolution process in §15 shall have all remedies available at law and equity. If a Purchasing Entity is in breach of a provision of an Order, Contractor shall have all remedies available to it under that Order and available at law and equity.

C. Purchasing Entity's Remedies

- i. If Contractor is in breach under any provision of an Order by a Purchasing Entity, the Purchasing Entity shall have all of the remedies listed in that Order, all remedies listed in §14. A. ii above, all remedies listed here in §14.C and all other remedies available by law or equity. The Purchasing Entity may exercise any or all of the remedies available to it, in its discretion, concurrently or consecutively.
- ii. If a Purchasing Entity gives Contractor notice of breach or terminates an Order because of Contractor's breach of that Order, Contractor shall provide notice to the State of that breach or termination within five Business Days following Contractor's receipt of that notice of breach or termination.
- iii. Payments and Damages

- a. Notwithstanding anything to the contrary, Purchasing Entities shall only pay Contractor for accepted Work received as of the date of termination. A Purchasing Entity may withhold any amount that may be due Contractor as the Purchasing Entity deems necessary until Contractor corrects its Work or to protect itself against loss including, without limitation, loss as a result of outstanding liens and costs incurred by the Purchasing Entity in procuring from third parties replacement Work as cover.
- b. Notwithstanding any other remedial action by the State, Contractor shall remain liable to the State or appropriate Purchasing Entity for any damages sustained by the State or Purchasing Entity in connection with any breach by Contractor, and the Purchasing Entity may withhold payment to Contractor for the purpose of mitigating the Purchasing Entity's damages.

A Purchasing Entity may deny payment to Contractor for Work not performed, or that due to Contractor's actions or inactions, cannot be performed or if they were performed are reasonably of no value to the state; provided, that any denial of payment shall be equal to the value of the obligations not performed.

15. DISPUTE RESOLUTION

A. Order Disputes, Termination and Resolution

- i. If a dispute related to an Order arises between Contractor and a Purchasing Entity, Contractor shall meet with the Purchasing Entity to attempt to resolve the issue. If Contractor is unable to resolve the issue with the Purchasing Entity, then Contractor may request assistance from the State by submitting a request in writing, which includes the pertinent information about the dispute and the assistance sought by Contractor, in accordance with §5 of the Participating Addendum. Nothing in this section shall be interpreted as limiting the rights or obligations of Contractor, the State or any Purchasing Entity under this Contract of any Order.
- ii. A Purchasing Entity may terminate an Order if it determines that Contractor was in breach of that Order. Termination of an Order shall not terminate any other Order or this Participating Addendum.
- iii. If a Purchasing Entity gives Contractor notice of breach or terminates an Order because of Contractor's breach of that Order, Contractor shall provide notice to the State of that breach or termination within five Business Days following Contractor's receipt of that notice of breach or termination.

B. Initial Resolution

Except as herein specifically provided otherwise, disputes concerning the performance of this Participating Addendum which cannot be resolved by the designated Participating Addendum primary contacts, as identified in §5 of the Participating Addendum, or through a dispute on an Order shall be referred in writing to a senior departmental management staff member designated by the State and a senior manager designated by Contractor for resolution.

C. Resolution of Controversies arising under this Participating Addendum

If the initial resolution described in §15.B fails to resolve the dispute within 10 Business Days, Contractor shall submit any alleged breach of this Participating Addendum by the State to the Procurement Official of the State Purchasing and Contracts Office as described in in §24-

101-301(30), C.R.S. for resolution in accordance with the provisions of §§24-109-101.1 through 24-109-505, C.R.S., (the "Resolution Statutes"), except that if Contractor wishes to challenge any decision rendered by the Procurement Official, Contractor's challenge shall be an appeal to the Executive Director of the Department of Personnel and Administration, or their delegate, under the Resolution Statutes before Contractor pursues any further action as permitted by such statutes. Except as otherwise stated in this Section, all requirements of the Resolution Statutes shall apply including, without limitation, time limitations.

16. RIGHTS IN WORK PRODUCT AND OTHER INFORMATION

A. Work Product

Contractor assigns to the Purchasing Entity and its successors and assigns, the entire right, title, and interest in and to all causes of action, either in law or in equity, for past, present, or future infringement of intellectual property rights related to the Work Product and all works based on, derived from, or incorporating the Work Product under an Order. Whether or not Contractor is under contract with the State at the time, Contractor shall execute applications, assignments, and other documents, and shall render all other reasonable assistance requested by the State, to enable the Purchasing Entity to secure patents, copyrights, licenses and other intellectual property rights related to the Work Product. To the extent that Work Product would fall under the definition of "works made for hire" under 17 U.S.C.S. §101, the parties intend the Work Product to be a work made for hire.

i. Copyrights

To the extent that the Work Product (or any portion of the Work Product) would not be considered works made for hire under applicable law, Contractor hereby assigns to the Purchasing Entity, the entire right, title, and interest in and to copyrights in all Work Product and all works based upon, derived from, or incorporating the Work Product; all copyright applications, registrations, extensions, or renewals relating to all Work Product and all works based upon, derived from, or incorporating the Work Product; and all moral rights or similar rights with respect to the Work Product throughout the world. To the extent that Contractor cannot make any of the assignments required by this section, Contractor hereby grants to the Purchasing Entity a perpetual, irrevocable, royalty-free license to use, modify, copy, publish, display, perform, transfer, distribute, sell, and create derivative works of the Work Product created under that Purchasing Entity's Order and all works based upon, derived from, or incorporating the Work Product by all means and methods and in any format now known or invented in the future. The Purchasing Entity may assign and license its rights under this license.

ii. Patents

In addition, Contractor grants to the Purchasing Entity (and to recipients of Work Product distributed by or on behalf of the State) a perpetual, worldwide, no-charge, royalty-free, irrevocable patent license to make, have made, use, distribute, sell, offer for sale, import, transfer, and otherwise utilize, operate, modify and propagate the contents of the Work Product created under an Order. Such license applies only to those patent claims licensable by Contractor that are necessarily infringed by the Work Product alone, or by the combination of the Work Product with anything else used by the Purchasing Entity.

iii. Assignments and Assistance

Whether or not Contractor is under contract with the State at the time, Contractor shall execute applications, assignments, and other documents, and shall render all other reasonable assistance requested by the State, to enable the State to secure patents, copyrights, licenses, and other intellectual property rights related to the Work Product. The Parties intend the Work Product to be works made for hire. Contractor assigns to the State and its successors and assigns, the entire right, title, and interest in and to all causes of action, either in law or in equity, for past, present, or future infringement of intellectual property rights related to the Work Product and all works based on, derived from, or incorporating the Work Product.

B. Exclusive Property of the State

Except to the extent specifically provided elsewhere in this Participating Addendum, any pre-existing State Records, State software, research, reports, studies, photographs, negatives or other documents, drawings, models, materials, data and information shall be the exclusive property of the State (collectively, "State Materials"). Contractor shall not use, willingly allow, cause or permit Work Product or State Materials to be used for any purpose other than the performance of Contractor's obligations in this Participating Addendum without the prior written consent of the State. Upon termination of this Participating Addendum for any reason, Contractor shall provide all Work Product and State Materials to the State in a form and manner as directed by the State.

C. Exclusive Property of Contractor

Contractor retains the exclusive rights, title, and ownership to any and all pre-existing materials owned or licensed to Contractor including, but not limited to, all pre-existing software, licensed products, associated source code, machine code, text images, audio and/or video, and third-party materials, delivered by Contractor under the Contract, whether incorporated in a Deliverable or necessary to use a Deliverable (collectively, "Contractor Property"). Contractor Property shall be licensed to the State as set forth in this Contract or a State approved license agreement: (i) entered into as exhibits to this Contract; (ii) obtained by the State from the applicable third-party vendor; or (iii) in the case of open source software, the license terms set forth in the applicable open source license agreement.

17. OBLIGATIONS AND RIGHTS IN THE EVENT OF TERMINATION OF ORDER OR CONTRACT

To the extent specified in any termination notice, Contractor shall not incur further obligations or render further performance past the effective date of such notice, and shall terminate outstanding orders and subcontracts with third parties. However, Contractor shall complete and deliver to Purchasing Entities all Work not cancelled by the termination notice, and may incur obligations as necessary to do so within this Participating Addendum's terms. At the request of the State, Contractor shall assign to the appropriate Purchasing Entity all of Contractor's rights, title, and interest in and to such terminated orders or subcontracts. Upon termination, Contractor shall take timely, reasonable and necessary action to protect and preserve property in the possession of Contractor in which the appropriate Purchasing Entity has an interest. At the State or Purchasing Entity's request, Contractor shall return materials owned by the Purchasing Entity that Contractor possesses at the time of any termination. Contractor shall deliver all completed Work Product to the appropriate Purchasing Entity at the State or Purchasing Entity's request.

18. STATEWIDE CONTRACT MANAGEMENT SYSTEM

If the maximum amount payable to Contractor under this Contract is \$100,000 or greater, either on the Effective Date or at any time thereafter, this section shall apply. Contractor agrees to be governed by and comply with the provisions of §§24-102-206, 24-106-103, 24-106-106, and 24-106-107, C.R.S. regarding the monitoring of vendor performance and the reporting of contract information in the State's contract management system ("Contract Management System" or "CMS"). Contractor's performance shall be subject to evaluation and review in accordance with the terms and conditions of this Contract, Colorado statutes governing CMS, and State Fiscal Rules and State Controller policies.

19. GENERAL PROVISIONS

A. Assignment

Contractor's rights and obligations under this Participating Addendum are personal and may not be transferred or assigned without the prior, written consent of the State. Any attempt at assignment or transfer without such consent shall be void. Any assignment or transfer of Contractor's rights and obligations approved by the State shall be subject to the provisions of this Participating Addendum.

B. Subcontracts

Contractor shall not enter into any subcontract in connection with its obligations under this Contract without the prior, written approval of the State. Contractor shall submit to the State a copy of each subcontract upon request by the State. All subcontracts entered into by Contractor in connection with this Participating Addendum shall comply with all applicable federal and state laws and regulations, shall provide that they are governed by the laws of the State of Colorado, and shall be subject to all provisions of this Participating Addendum.

C. Binding Effect

Except as otherwise provided in §19.A., all provisions of this Participating Addendum, including the benefits and burdens, shall extend to and be binding upon the Parties' respective successors and assigns.

D. Authority

Each Party represents and warrants to the other that the execution and delivery of this Participating Addendum and the performance of such Party's obligations have been duly authorized.

E. Captions and References

The captions and headings in this Participating Addendum are for convenience of reference only, and shall not be used to interpret, define, or limit its provisions. All references in this Participating Addendum to sections (whether spelled out or using the § symbol), subsections, exhibits or other attachments, are references to sections, subsections, exhibits or other attachments contained herein or incorporated as a part hereof, unless otherwise noted.

F. Counterparts

This Participating Addendum may be executed in multiple, identical, original counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute the same agreement.

G. Entire Understanding

This Participating Addendum represents the complete integration of all understandings between the Parties related to the Work, and all prior representations and understandings related to the Work, oral or written, are merged into this Participating Addendum. Prior or contemporaneous additions, deletions, or other changes to this Participating Addendum shall not have any force or effect whatsoever, unless embodied herein.

H. Digital Signatures

If any signatory signs this agreement using a digital signature in accordance with the Colorado State Controller Contract, Grant and Purchase Order Policies regarding the use of digital signatures issued under the State Fiscal Rules, then any agreement or consent to use digital signatures within the electronic system through which that signatory signed shall be incorporated into this Contract by reference.

I. Modification

Except as otherwise provided in this Participating Addendum, any modification to this Participating Addendum shall only be effective if agreed to in a formal amendment to this Participating Addendum, properly executed and approved in accordance with applicable Colorado State law and State Fiscal Rules. Modifications permitted under this Participating Addendum, other than contract amendments, shall conform to the policies issued by the Colorado State Controller.

J. Statutes, Regulations, Fiscal Rules, and Other Authority.

Any reference in this Participating Addendum to a statute, regulation, State Fiscal Rule, fiscal policy or other authority shall be interpreted to refer to such authority then current, as may have been changed or amended since the Effective Date of this Participating Addendum.

K. Severability

The invalidity or unenforceability of any provision of this Participating Addendum shall not affect the validity or enforceability of any other provision of this Participating Addendum, which shall remain in full force and effect, if the Parties can continue to perform their obligations under this Participating Addendum in accordance with the intent of this Participating Addendum.

L. Survival of Certain Contract Terms

Any provision of this Participating Addendum that imposes an obligation on the Contractor or a Purchasing Entity after termination or expiration of this Participating Addendum shall survive the termination or expiration of this Participating Addendum and shall be enforceable by the other Party.

M. Taxes

The State is exempt from federal excise taxes under I.R.C. Chapter 32 (26 U.S.C., Subtitle D, Ch. 32) (Federal Excise Tax Exemption Certificate of Registry No. 84-730123K) and from State and local government sales and use taxes under §§39-26-704(1), *et seq.*, C.R.S. (Colorado Sales Tax Exemption Identification Number 98-02565). The State shall not be liable for the payment of any excise, sales, or use taxes, regardless of whether any political subdivision of the State imposes such taxes on Contractor. Contractor shall be solely responsible for any exemptions from the collection of excise, sales or use taxes that Contractor may wish to have in place in connection with this Participating Addendum. Contractor shall honor any tax exemption that any Purchasing Entity has, and shall not charge

any Purchasing Entity any excise, sales, or use taxes from which that Purchasing Entity is exempt.

N. Third Party Beneficiaries

Except for a Purchasing Entity and/or the Parties' respective successors and assigns described in §19.A, this Participating Addendum does not and is not intended to confer any rights or remedies upon any person or entity other than the Parties. Enforcement of this Participating Addendum and all rights and obligations hereunder are reserved solely to the Parties. Any services or benefits which third parties receive as a result of this Participating Addendum are incidental to this Participating Addendum, and do not create any rights for such third parties.

O. Waiver

A Party's failure or delay in exercising any right, power, or privilege under this Participating Addendum, whether explicit or by lack of enforcement, shall not operate as a waiver, nor shall any single or partial exercise of any right, power, or privilege preclude any other or further exercise of such right, power, or privilege.

P. CORA Disclosure

To the extent not prohibited by federal law, this Participating Addendum and the performance measures and standards required under §24-106-107, C.R.S., if any, are subject to public release through the CORA.

Q. Standard and Manner of Performance

Contractor shall perform its obligations under this Participating Addendum in accordance with the highest standards of care, skill and diligence in Contractor's industry, trade, or profession.

R. Licenses, Permits, and Other Authorizations.

Contractor shall secure, prior to the Effective Date, and maintain at all times during the term of this Participating Addendum, at its sole expense, all licenses, certifications, permits, and other authorizations required to perform its obligations under this Participating Addendum, and shall ensure that all employees, agents and Subcontractors secure and maintain at all times during the term of their employment, agency or subcontract, all license, certifications, permits and other authorizations required to perform their obligations in relation to this Participating Addendum.

S. Indemnification

i. General Indemnification

Contractor shall indemnify, save, and hold harmless the State, its employees, agents and assignees (the "Indemnified Parties"), against any and all costs, expenses, claims, damages, liabilities, court awards and other amounts (including attorneys' fees and related costs) incurred by any of the Indemnified Parties in relation to any act or omission by Contractor, or its employees, agents, Subcontractors, or assignees in connection with this Participating Addendum.

ii. Confidential Information Indemnification

Disclosure or use of State Confidential Information by Contractor in violation of §10 may be cause for legal action by third parties against Contractor, the State, or their respective agents. Contractor shall indemnify, save, and hold harmless the Indemnified

Parties, against any and all claims, damages, liabilities, losses, costs, expenses (including attorneys' fees and costs) incurred by the State in relation to any act or omission by Contractor, or its employees, agents, assigns, or Subcontractors in violation of §10.

iii. **Intellectual Property Indemnification**

Contractor shall indemnify, save, and hold harmless the Indemnified Parties, against any and all costs, expenses, claims, damages, liabilities, and other amounts (including attorneys' fees and costs) incurred by the Indemnified Parties in relation to any claim that any Deliverable, Good or Service, software, or Work Product provided by Contractor under this Contract (collectively, "IP Deliverables"), or the use thereof, infringes a patent, copyright, trademark, trade secret, or any other intellectual property right. Contractor's obligations hereunder shall not extend to the combination of any IP Deliverables provided by Contractor with any other product, system, or method, unless the other product, system, or method is (a) provided by Contractor or Contractor's subsidiaries or affiliates; (b) specified by Contractor to work with the IP Deliverables; (c) reasonably required in order to use the IP Deliverables in its intended manner and the infringement could not have been avoided by substituting another reasonably available product, system, or method capable of performing the same function; or (d) is reasonably expected to be used in combination with the IP Deliverables.

20. COLORADO SPECIAL PROVISIONS (COLORADO FISCAL RULE 3-3)

These Special Provisions apply to all contracts except where noted in italics.

A. STATUTORY APPROVAL. §24-30-202(1), C.R.S.

This Contract shall not be valid until it has been approved by the Colorado State Controller or designee. If this Contract is for a Major Information Technology Project, as defined in §24-37.5-102(2.6), then this Contract shall not be valid until it has been approved by the State's Chief Information Officer or designee.

B. FUND AVAILABILITY. §24-30-202(5.5), C.R.S.

Financial obligations of the State payable after the current State Fiscal Year are contingent upon funds for that purpose being appropriated, budgeted, and otherwise made available.

C. GOVERNMENTAL IMMUNITY.

Liability for claims for injuries to persons or property arising from the negligence of the State, its departments, boards, commissions committees, bureaus, offices, employees and officials shall be controlled and limited by the provisions of the Colorado Governmental Immunity Act, §24-10-101, et seq., C.R.S.; the Federal Tort Claims Act, 28 U.S.C. Pt. VI, Ch. 171 and 28 U.S.C. 1346(b), and the State's risk management statutes, §§24-30-1501, et seq. C.R.S. No term or condition of this Contract shall be construed or interpreted as a waiver, express or implied, of any of the immunities, rights, benefits, protections, or other provisions, contained in these statutes.

D. INDEPENDENT CONTRACTOR

Contractor shall perform its duties hereunder as an independent contractor and not as an employee. Neither Contractor nor any agent or employee of Contractor shall be deemed an agent or employee of the State. Contractor shall not have authorization, express or implied,

to bind the State to any agreement, liability or understanding, except as expressly set forth herein. **Contractor and its employees and agents are not entitled to unemployment insurance or workers compensation benefits through the State and the State shall not pay for or otherwise provide such coverage for Contractor or any of its agents or employees. Contractor shall pay when due all applicable employment taxes, income taxes, and local head taxes incurred pursuant to this Contract. Contractor shall (i) provide and keep in force workers' compensation and unemployment compensation insurance in the amounts required by law, (ii) provide proof thereof when requested by the State, and (iii) be solely responsible for its acts and those of its employees and agents.**

E. COMPLIANCE WITH LAW.

Contractor shall comply with all applicable federal and State laws, rules, and regulations in effect or hereafter established, including, without limitation, laws applicable to discrimination and unfair employment practices.

F. CHOICE OF LAW, JURISDICTION, AND VENUE.

Colorado law, and rules and regulations issued pursuant thereto, shall be applied in the interpretation, execution, and enforcement of this Contract. Any provision included or incorporated herein by reference, which conflicts with said laws, rules, and regulations shall be null and void. All suits or actions related to this Contract shall be filed and proceedings held in the State of Colorado and exclusive venue shall be in the City and County of Denver.

G. PROHIBITED TERMS.

Any term included in this Contract that requires the State to indemnify or hold Contractor harmless; requires the State to agree to binding arbitration; limits Contractor's liability for damages resulting from death, bodily injury, or damage to tangible property; or that conflicts with this provision in any way shall be void ab initio. Nothing in this Contract shall be construed as a waiver of any provision of §24-106-109 C.R.S. Any term included in this Contract that limits Contractor's liability that is not void under this section shall apply only in excess of any insurance to be maintained under this Contract, and no insurance policy shall be interpreted as being subject to any limitations of liability of this Contract.

H. SOFTWARE PIRACY PROHIBITION.

State or other public funds payable under this Contract shall not be used for the acquisition, operation, or maintenance of computer software in violation of federal copyright laws or applicable licensing restrictions. Contractor hereby certifies and warrants that, during the term of this Contract and any extensions, Contractor has and shall maintain in place appropriate systems and controls to prevent such improper use of public funds. If the State determines that Contractor is in violation of this provision, the State may exercise any remedy available at law or in equity or under this Contract, including, without limitation, immediate termination of this Contract and any remedy consistent with federal copyright laws or applicable licensing restrictions.

I. EMPLOYEE FINANCIAL INTEREST/CONFLICT OF INTEREST. §§24-18-201 and 24-50-507, C.R.S.

The signatories aver that to their knowledge, no employee of the State has any personal or beneficial interest whatsoever in the service or property described in this Contract. Contractor has no interest and shall not acquire any interest, direct or indirect, that would conflict in any

manner or degree with the performance of Contractor's services and Contractor shall not employ any person having such known interests.

J. VENDOR OFFSET AND ERRONEOUS PAYMENTS. §§24-30-202(1) and 24-30-202.4, C.R.S.

[Not applicable to intergovernmental agreements] Subject to §24-30-202.4(3.5), C.R.S., the State Controller may withhold payment under the State's vendor offset intercept system for debts owed to State agencies for: (i) unpaid child support debts or child support arrearages; (ii) unpaid balances of tax, accrued interest, or other charges specified in §§39-21-101, *et seq.*, C.R.S.; (iii) unpaid loans due to the Student Loan Division of the Department of Higher Education; (iv) amounts required to be paid to the Unemployment Compensation Fund; and (v) other unpaid debts owing to the State as a result of final agency determination or judicial action. The State may also recover, at the State's discretion, payments made to Contractor in error for any reason, including, but not limited to, overpayments or improper payments, and unexpended or excess funds received by Contractor by deduction from subsequent payments under this Contract, deduction from any payment due under any other contracts, grants or agreements between the State and Contractor, or by any other appropriate method for collecting debts owed to the State.

K. PUBLIC CONTRACTS FOR SERVICES. §§8-17.5-101, *et seq.*, C.R.S.

[Not applicable to agreements relating to the offer, issuance, or sale of securities, investment advisory services or fund management services, sponsored projects, intergovernmental agreements, or information technology services or products and services] Contractor certifies, warrants, and agrees that it does not knowingly employ or contract with an illegal alien who will perform work under this Contract and will confirm the employment eligibility of all employees who are newly hired for employment in the United States to perform work under this Contract, through participation in the E-Verify Program or the State verification program established pursuant to §8-17.5-102(5)(c), C.R.S., Contractor shall not knowingly employ or contract with an illegal alien to perform work under this Contract or enter into a contract with a Subcontractor that fails to certify to Contractor that the Subcontractor shall not knowingly employ or contract with an illegal alien to perform work under this Contract. Contractor (i) shall not use E-Verify Program or the program procedures of the Colorado Department of Labor and Employment ("Department Program") to undertake pre-employment screening of job applicants while this Contract is being performed, (ii) shall notify the Subcontractor and the contracting State agency or institution of higher education within 3 days if Contractor has actual knowledge that a Subcontractor is employing or contracting with an illegal alien for work under this Contract, (iii) shall terminate the subcontract if a Subcontractor does not stop employing or contracting with the illegal alien within 3 days of receiving the notice, and (iv) shall comply with reasonable requests made in the course of an investigation, undertaken pursuant to §8-17.5-102(5), C.R.S., by the Colorado Department of Labor and Employment. If Contractor participates in the Department program, Contractor shall deliver to the contracting State agency, Institution of Higher Education or political subdivision, a written, notarized affirmation, affirming that Contractor has examined the legal work status of such employee, and shall comply with all of the other requirements of the Department program. If Contractor fails to comply with any requirement of this provision or §§8-17.5-101, *et seq.*, C.R.S., the contracting State agency, institution of higher education or political subdivision may terminate this Contract for breach and, if so terminated, Contractor shall be liable for damages.

L. PUBLIC CONTRACTS WITH NATURAL PERSONS. §§24-76.5-101, *et seq.*, C.R.S.

Contractor, if a natural person eighteen (18) years of age or older, hereby swears and affirms under penalty of perjury that Contractor (i) is a citizen or otherwise lawfully present in the United States pursuant to federal law, (ii) shall comply with the provisions of §§24-76.5-101, *et seq.*, C.R.S., and (iii) has produced one form of identification required by §24-76.5-103, C.R.S. prior to the Effective Date of this Contract.

EXHIBIT B STATEMENT OF WORK

1. GOODS AND/OR SERVICES

For a description of what the Participating Addendum will provide, see Exhibits 1, 2 and 3 of the Master Agreement AR3102, "Cloud Solutions"

2. OTHER PROJECT REQUIREMENTS

A. Delivery of Goods and Performance of Services

- i. Contractor shall provide all Goods and perform all Services described in each Order.
- ii. Unless specifically agreed to otherwise in an Order, Contractor shall deliver all Goods under an Order in good, working and undamaged condition. All Goods shall be free on board ("F.O.B.") destination to the location specified in the Order.
- iii. If a good in an Order is out of stock, Contractor may only provide a substitute good if it has notified the Purchasing Entity for that Order, in writing, that the good is out of stock and has received the Purchasing Entity's approval to provide the substitute good. Purchasing Entities may request additional information comparing the substitute good with the original good in the Purchasing Entity's sole discretion.

B. Additional Terms

Any additional terms and conditions on any invoice, statement, Contractor time sheet, website, electronic license or use agreement or any other form, including, without limitation, terms regarding indemnification, limitation of liability, cancellation fees, choice of law and binding arbitration shall be void and unenforceable except to the extent that they are specifically included in this Participating Addendum or an Order. The signature of any employee of a Purchasing Entity on any such form shall be effective to establish receipt of Goods or completion of Services and shall not make any term of that form enforceable.

EXHIBIT C PRODUCTS AND PRICE LIST

1. Contractor has been awarded the following categories:

- CLOUD SOLUTIONS

2. The products and price list is located on the Contractor's dedicated State website, hosted and maintained by the Contractor, and is incorporated into this Participating Addendum by reference. Changes in product and pricing must be approved by the lead state and shall be effective when published on the dedicated state website.

Contractor's website address

3. Pricing

A. Price Lists

The State may publish any pricing information under this Participating Addendum, including, without limitation the pricing information shown in this **Exhibit C, Products and Price List**, on the State's website and any other website as the State determines is necessary or efficient to facilitate the use of this Participating Addendum by Purchasing Entities.

B. Price Decreases and Ceiling Prices

The prices listed in this **Exhibit C** are Ceiling Prices, and Contractor may offer lower prices to Purchasing Entities, and Purchasing Entities may negotiate lower prices with Contractor, without the review or approval of the State. Contractor shall not allow a Subcontractor to charge an amount greater than the Ceiling Price for any Order.

C. Environmentally Preferable Purchasing

- Contractor shall provide training regarding the environmentally preferable products, as defined in the State's Environmentally Preferable Purchasing Policy, that are purchased or made available under this Participating Addendum. This training shall be provided at no additional cost, unless otherwise agreed upon by the Parties, and shall be presented at a time and in a manner as agreed upon by the Parties.
- The State reserves the right to request additional provisions and requirements to ensure this Participating Addendum is in compliance with all State regulations and policies, including all sustainable purchasing and environmentally preferable purchasing policies or executive orders.

Exhibit C



1. NASPO Pricing Notes and Explanations

GTRI is pleased to provide the State of Utah with its pricing response to Bid #: SK18008. The attached NASPO Pricing offers pricing for the following Cloud Models: IaaS, and PaaS.

GTRI is a leading provider of Cloud Solutions and Services to the Public Sector and a leading delivery and resale partner for Amazon Web Services (AWS). Our distinct capabilities and qualifications include the following:

- AWS Advanced Public Sector Partner
- Exceptional cybersecurity as demonstrated by Cloud Security Alliance (CSA) Assessments
- ISO 9001, certifications
- Agile project delivery

The following consulting services and solutions are available:

- Section 1: Professional Services and access to AWS Professional Services
- Section 2: Managed Service Provider (MSP) offerings backed by a rigorous AWS audit process
- Section 3: Resale of the full AWS IaaS catalog
- Section 4: AWS Marketplace and related offerings
- Section 5: Pricing and rate card for consulting services

1.1. Professional Services

GTRI is one of the leading public sector providers of cloud professional services. Our highly qualified, AWS-certified consultants have extensive experience in cloud solutions, including transition from legacy environments, migration of workloads, and optimization in the cloud. Services can be tailored to individual customer requirements and will be priced according to those requirements using the appropriate labor rates as listed in Section 5. Services can also be delivered through GTRI by AWS-badged consultants (AWS Professional Services).

Service Name	Description	Service Model	Deployment Model	Pricing
Cloud Services Assessment and Proof of Concept	Partner with Customer to identify requirements for a proof of concept system and translate those requirements into a functional prototype, demonstrate potential ROI, and provide models for total cost of ownership (TCO). Includes Discovery Workshops to gather business and technical requirements within the scope of the CSP platform.	IaaS	All (Public, Private, Hybrid, Community)	See rate card (Section 5)
Architecture and Design	Conduct planning and create technical architecture and design documents for cloud services capabilities using industry best practices.	IaaS	All (Public, Private, Hybrid, Community)	See rate card (Section 5)
Provisioning and	All services required for the provisioning of cloud services as defined by purchase order	IaaS	All (Public, Private,	See rate card



Service Name	Description	Service Model	Deployment Model	Pricing
Development	requirements. Provision cloud environments for production, integration, development, and sandbox purposes to support the complete systems lifecycle. Provisioning and development capabilities include but are not limited to: systems development services; software development services; cloud development services; development and testing platform provision services; tools and applications development services; configuration and change management services.		Hybrid, Community)	(Section 5)
Migration, Deployment, and Optimization	All support operations necessary to fully migrate and deploy Customer target applications and services to the cloud. Accommodate enterprise considerations such as impact on Customer operating units, contracts, management, and technical components (e.g. application, infrastructure, and security). Provide communications plans for all affected parties of the migration(s) to ensure end-user adoption, customer satisfaction, successful organizational process changes, and alignment with Customer policies, requirements and goals. Additional capabilities include but are not limited to: Assistance with software license mobility and migration status reporting (e.g. milestone and migration test plans and related rollback capabilities and plans).	IaaS	All (Public, Private, Hybrid, Community)	See rate card (Section 5)
Application Optimization	Full software development lifecycle services for both legacy on premise application workloads and new application solutions deployed in the CSP platform and optimized/refactored for a cloud utility model. This includes application design following an agile methodology and framework to utilize such cloud features as effective load balancing, auto scaling, high availability, security, elastic storage, and on-demand provisioning. Activities include requirements gathering, design, deployment, configuration, user acceptance testing, compliance, and ongoing support.	IaaS	All (Public, Private, Hybrid, Community)	See rate card (Section 5)



Service Name	Description	Service Model	Deployment Model	Pricing
Cloud Customer Support	U.S. based, U.S. Citizen 24x7 Cloud Customer Support help desk services including web, email, and phone support. The support framework includes knowledge capture and sharing, enabling trusted communications, timely response and appropriate escalation, performance management and reporting, and the ability to reach back to CSP support.	IaaS	All (Public, Private, Hybrid, Community)	See rate card (Section 5)
Training	System administrator, user, and power user level training covering architecture, basics and essentials, and system administration or operations. Available delivery mechanisms include classroom delivery at the Government or Contractor site.	IaaS	All (Public, Private, Hybrid, Community)	See rate card (Section 5)
Service Level Management	SLAs for management and delivery of contracted cloud services. This includes standard industry metrics and measures for establishing performance levels for each service, or relevant service component. Service Level Management includes, but is not limited to: SLA response time and resolution/mitigation time; Service level monitoring, reporting and notification of a failure to meet SLAs; SLA Enforcement Mechanisms (e.g. service credit, etc.); Key performance indicators/metrics; Service level reports (real-time and historical) to track service health, status, usage, volume of trouble calls, resource utilization, change metrics, security status, etc.	IaaS	All (Public, Private, Hybrid, Community)	See rate card (Section 5)
Quality Assurance and Quality Control	Quality Assurance and Quality Controls are integrated into all aspects of service delivery. Available deliverables include a Quality Assurance Surveillance Plan (QASP) and/or Quality Control Plan (QCP) that includes details for measuring performance and deliverables with metrics that may include data availability, storage capacity, uptime, etc. These documents are correlated with the "as-is" and "to-be" environments as defined in contract requirements.	IaaS	All (Public, Private, Hybrid, Community)	See rate card (Section 5)



Service Name	Description	Service Model	Deployment Model	Pricing
Security and Compliance	Robust security design, configuration, and support focused on the integration points of end-user authentication (e.g. SAML, AD, LDAP), cloud environment management authentication, and physical and logical security and certification, audit and logging, etc. Subject matter expertise and assistance in documenting controls and obtaining the authority to operate based on applicable standards and security controls.	IaaS	All (Public, Private, Hybrid, Community)	See rate card (Section 5)
Program and Project Management Support	Routine program and project management is available for all professional services and managed services. This includes regular meetings with customer leadership to review the following: progress, problems encountered, completed tasks, in-process tasks, upcoming tasks, management metrics, program budgets, status of deliverables, status of project timelines, and staffing plans. These management functions will be outlined in a contractor- provided Project Management Plan that also identifies key metrics that will be used to measure success.	IaaS	All (Public, Private, Hybrid, Community)	See rate card (Section 5)

1.2. Managed Service Provider (MSP) for PaaS Solution

Under the MSP model, GTRI assumes responsibility for a combination of underlying IaaS services and manages them under a Service Level Agreement (SLA). This combines the benefits of utility cloud computing with expert cloud architect, systems administration, and security consulting services as well as software licensing and professional consulting services. MSP services are billed as a combined offering on a per unit basis, generally per hour that the underlying cloud service is used. MSP services yield material cost savings because the end customer is only charged for the services they use.

GTRI offers the bundled MSP services as a rate per AWS price.

Service Name	Price
MSP Bundle	35%

This Managed services bundle includes the below services:



Managed Services Bundle	IaaS	PaaS
EC2 Instance Management	✓	✓
VPC and IP Management		
Storage Management	✓	✓
Database Management		
Backup Management	✓	✓
Billing and invoice management		
Project Deliverables	✓	✓
Continuous monitoring and support		
Reporting	✓	✓
User and Permission Management		
Cross Account Access Security	✓	✓
Firewall/NACL Management		
Operating System Hardening at Deployment	✓	✓
OS STIG Compliance (Web browser, Web Server)		
STIG Compliance Updates	✓	✓
Operating System Patching		
Monthly Vulnerability Scans	✓	✓
Vulnerability & Compliance Remediation and Troubleshooting		
Continuous Monitoring Dashboard	✓	✓
Anti-Virus / Anti-Malware Management		
Backups & Snapshots	✓	✓
SSP Documentation Support		
Log Retention and Archiving (CloudWatch)	✓	✓

In addition to the MSP bundle above, the following managed services can be purchased on an hourly T&M basis:



Service Name	Description	Service Model	Deployment Models	Pricing
Cloud Patch and Stack Management	Patch management is one of the core services under managed service delivery. GTRI will maintain in scope customer applications in a consistent secure state, including all software licensing, maintenance, and regular patching of the system so that updates are applied within 30 days of release. Mature, repeatable processes are used to conduct major and minor updates from operating system patches to hosted application updates. These processes are invoked following each of the following migration activities: Baseline creation, Baseline Updates, Stack Deployment, Testing, and Migration.	IaaS	All (Public, Private, Hybrid, Community)	See rate card (Section 5)
Cloud Log File Management	Maintain an audit record of system activity so that system logs can be analyzed and reviewed for security, application tuning, and troubleshooting. These logs are provided in centralized repository for viewing and analysis, which decreases the labor required to complete tasks.	IaaS	All (Public, Private, Hybrid, Community)	See rate card (Section 5)
Cloud Customer Support	Support for System Owners, Managers, and Administrators to assist with incident management and troubleshooting. This falls under the Service Operation process area of an ITIL-based service delivery framework and includes Incident, Problem, and Knowledge Management along with Service Request Fulfillment. Support is provided by an Help Desk maintained by U.S. citizens and located in the United States. Representatives are available by phone, email and self-service web portal 24x7x365.	IaaS	All (Public, Private, Hybrid, Community)	See rate card (Section 5)
Cloud Administrative Capabilities	Capabilities to assist the customer with maintaining the integrity of the system baseline through configuration and change control processes. As part of Service Transition under an ITIL-based service delivery framework, this includes assessing, reviewing, approving, scheduling, and testing all modifications to the system baseline before introducing the modification to the production environment. These capabilities also include managing an internal Change Advisory Board that assists the	IaaS	All (Public, Private, Hybrid, Community)	See rate card (Section 5)



Service Name	Description	Service Model	Deployment Models	Pricing
	customer with risk assessments, impact analysis, and other reviews.			
Cloud Data Archival	Maintain backup and recovery; identify specific data to retain in archive beyond standard backup retention windows for regulatory compliance or historical queries. This includes logs, databases, and static content.	IaaS	All (Public, Private, Hybrid, Community)	See rate card (Section 5)
Cloud Usage Support	CloudCheckr provides online reporting capabilities and a single pane of glass for customers to track system usage and associated costs. CloudCheckr seamlessly manages multiple accounts through a single interface, including account hierarchy, permissions, and cost allocation per organization. CloudCheckr also provides a centralized capability to perform resource level tagging with a standardized set of key value pairs across multiple accounts.	IaaS	All (Public, Private, Hybrid, Community)	See rate card (Section 5)
Cloud Administration Capabilities	Detailed reporting of server performance at up to one (1) minute reporting intervals. This provides near real-time insight into the status of every asset within the cloud environment.	IaaS	All (Public, Private, Hybrid, Community)	See rate card (Section 5)
Cloud Comprehensive Backup	Backup and recovery solutions to minimize data loss in the event of a service interruption while ensuring data integrity and removing single points of failure. Includes pre-architected solutions that leverage native CSP capabilities focused on servers, databases, and static content.	IaaS	All (Public, Private, Hybrid, Community)	See rate card (Section 5)
Splunk Logging Services	With Splunk, the entire environment can be developed into a continuous monitored environment with dashboards and alerts to integrate with a SIEM.	IaaS	All (Public, Private, Hybrid, Community)	See rate card (Section 5)

1.3. Infrastructure as a Service (IaaS) Offerings

GTRI currently has more than 50 distinct IaaS Offerings available from AWS. NASPO ValuePoint customers are guaranteed a minimum 2% discount from the current, real-time AWS list price for IaaS offerings. The current list prices are published on AWS public website.



Service Name	Description	Service Model	Deployment Models	Pricing
Amazon Elastic Compute Cloud (Amazon EC2)	Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable computing capacity—literally, servers in Amazon’s data centers—that you use to build and host your software systems.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
Amazon EC2 Container Service	Amazon EC2 Container Service is a highly scalable, high-performance container management service that supports Docker containers and allows you to easily run distributed applications on a managed cluster of Amazon EC2 instances.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
AWS Lambda	AWS Lambda is a compute service that runs your code in response to events and automatically manages the compute resources for you, making it easy to build applications that respond quickly to new information. AWS Lambda starts running your code within milliseconds of an event such as an image upload, in-app activity, website click, or output from a connected device.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
AWS Auto Scaling	Auto Scaling is a web service designed to launch or terminate Amazon EC2 instances automatically based on user-defined policies, schedules, and health checks.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
AWS Elastic Load Balancing	Elastic Load Balancing automatically distributes your incoming application traffic across multiple Amazon EC2 instances. It detects unhealthy instances and reroutes traffic to healthy instances until the unhealthy instances have been restored. Elastic Load Balancing automatically scales its request handling capacity in response to incoming traffic.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
Amazon VPC	Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you have defined. This virtual network closely resembles a traditional network that you would operate in your own data center, with the benefits of using the scalable infrastructure of AWS.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
Amazon Route 53	Amazon Route 53 is a highly available and scalable Domain Name System (DNS) web service.	IaaS	All (Public, Private, Hybrid,	Minimum 2%



Service Name	Description	Service Model	Deployment Models	Pricing
			Community)	discount off list price
AWS Direct Connect	AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard 1 GB or 10 GB Ethernet fiber optic cable. One end of the cable is connected to your router and the other to an AWS Direct Connect router. With this connection, you can create virtual interfaces directly to the AWS cloud and Amazon VPC, bypassing Internet service providers in your network path.	IaaS	AWS Direct Connect	Minimum 2% discount off list price
Amazon S3	Amazon Simple Storage Service (Amazon S3) is storage for the Internet. You can use Amazon S3 to store and retrieve any amount of data, at any time, from anywhere on the web. You can accomplish these tasks using the simple and intuitive web interface of the AWS Management Console.	IaaS	Amazon S3	Minimum 2% discount off list price
Amazon Glacier	Amazon Glacier is a storage service optimized for infrequently used data, or "cold data." The service provides secure, durable, and extremely low-cost storage for data archiving and backup. With Amazon Glacier, you can store your data cost effectively for months, years, or even decades. Amazon Glacier enables you to offload the administrative burdens of operating and scaling storage to AWS, so you do not have to worry about capacity planning, hardware provisioning, data replication, hardware failure detection and recovery, or time-consuming hardware migrations.	IaaS	Amazon Glacier	Minimum 2% discount off list price
Amazon EBS	Amazon Elastic Block Store (Amazon EBS) provides block-level storage volumes for use with Amazon EC2 instances. Amazon EBS volumes are highly available and reliable storage volumes that can be attached to any running instance that is in the same Availability Zone. Amazon EBS volumes that are attached to an Amazon EC2 instance are exposed as storage volumes that persist independently from the life of the instance. With Amazon EBS, you only pay for what you use.	IaaS	Amazon EBS	Minimum 2% discount off list price



Service Name	Description	Service Model	Deployment Models	Pricing
Amazon CloudFront	Amazon CloudFront is a content delivery web service. It integrates with other AWS cloud services to give developers and businesses an easy way to distribute content to end users with low latency, high data transfer speeds, and no commitments.	IaaS	Amazon CloudFront	Minimum 2% discount off list price
AWS Import/Export	AWS Import/Export accelerates transferring large amounts of data between the cloud and portable storage devices that you mail to us. AWS transfers data directly onto and off your storage devices using Amazon's high-speed internal network. Data load typically begins the next business day after the storage device arrives at AWS. After the data export or import completes, we return the storage device. For large data sets, AWS Import/Export is significantly faster than Internet transfer and more cost effective than upgrading your connectivity.	IaaS	AWS Import/Export	Minimum 2% discount off list price
AWS Storage Gateway	AWS Storage Gateway is a service that connects an on premises software appliance with cloud-based storage to provide seamless and secure integration between your on premises IT environment and AWS's storage infrastructure.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
Amazon RDS	Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to set up, operate, and scale a relational database in the cloud. It provides cost-efficient, resizable capacity for an industry-standard relational database and manages common database administration tasks. Database engines available through Amazon RDS include Amazon Aurora, MySQL, Oracle, Microsoft SQL Server, and PostgreSQL.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
Amazon Dynamo DB	Amazon DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. You can use Amazon DynamoDB to create a database table that can store and retrieve any amount of data and serve any level of request traffic. Amazon DynamoDB automatically spreads the data and traffic for the table over a sufficient number of servers to handle the request capacity specified by the customer and the amount of data stored, while maintaining consistent and fast performance.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price



Service Name	Description	Service Model	Deployment Models	Pricing
Amazon Redshift	Amazon Redshift is a fast, fully managed, petabyte-scale data warehouse solution that makes it simple and cost-effective to efficiently analyze all your data using your existing business intelligence tools. You can start small with no commitments and scale to a petabyte or more.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
Amazon ElastiCache	Amazon ElastiCache is a web service that makes it easy to set up, manage, and scale distributed, in-memory cache environments in the cloud. It provides a high-performance, resizable, and cost-effective in-memory cache, while removing the complexity associated with deploying and managing a distributed cache environment.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
Amazon Elastic MapReduce	Amazon Elastic MapReduce (Amazon EMR) is a web service that makes it easy to process large amounts of data efficiently. Amazon EMR uses Hadoop processing combined with several AWS products to perform such tasks as web indexing, data mining, log file analysis, machine learning, scientific simulation, and data warehousing.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
Amazon Kinesis	Amazon Kinesis is a managed service that scales elastically for real-time processing of streaming big data. The service takes in large streams of data records that can then be consumed in real time by multiple data processing applications that can be run on Amazon EC2 instances. The data processing applications use the Amazon Kinesis Client Library and are called "Amazon Kinesis applications."	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
AWS Data Pipeline	AWS Data Pipeline is a web service that helps you reliably process and move data between different AWS compute and storage services as well as on premises data sources at specified intervals. With AWS Data Pipeline, you can regularly access your data where it is stored, transform and process it at scale, and efficiently transfer the results to AWS cloud services such as Amazon S3, Amazon RDS, Amazon DynamoDB, and Amazon EMR.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
Amazon Mobile Analytics	Amazon Mobile Analytics is a service that lets you easily collect, visualize, and understand application usage data at scale. Many mobile application analytics solutions deliver usage data	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2%



Service Name	Description	Service Model	Deployment Models	Pricing
	several hours after the events occur. Amazon Mobile Analytics is designed to deliver usage reports within 60 minutes of receiving data from an application so that you can act on the data more quickly.			discount off list price
AWS Identity & Access Management (IAM)	AWS (IAM) is a web service that enables AWS customers to manage users and user permissions in AWS. The service is targeted at organizations with multiple users or systems that use AWS products such as Amazon EC2, Amazon SimpleDB, and the AWS Management Console. With AWS IAM, you can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
AWS Directory Service	AWS Directory Service is a managed service that allows customers to connect their AWS resources with an existing on-premises Microsoft Active Directory or to set up a new, standalone directory in the AWS Cloud. Connecting to an on-premises directory is easy, and when this connection is established, all users can access AWS resources and applications with their existing corporate credentials.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
AWS Service Catalog	AWS Service Catalog is a service that allows administrators to create and manage approved catalogs of resources that end users can then access via a personalized portal. You can control which users have access to which applications or AWS resources to enable compliance with your business policies, while users can easily browse and launch products from the catalogs.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
AWS Config	AWS Config is a fully managed service that provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance. With AWS Config you can discover existing AWS resources, export a complete inventory of your AWS resources with all configuration details, and determine how a resource was configured at any point in time. These capabilities enable compliance auditing, security analysis, resource change tracking, and troubleshooting.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price



Service Name	Description	Service Model	Deployment Models	Pricing
AWS CloudHSM	AWS CloudHSM provides secure cryptographic key storage to customers by making Hardware Security Modules (HSMs) available in the AWS cloud.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
AWS Key Management Service	AWS Key Management Service (KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data and uses Hardware Security Modules (HSMs) to protect the security of your keys. AWS KMS is integrated with other AWS cloud services including Amazon EBS, Amazon S3, and Amazon Redshift. AWS KMS is also integrated with AWS CloudTrail to provide you with logs of all key usage to help meet your regulatory and compliance needs.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
AWS CloudTrail	With AWS CloudTrail, customers can get a history of AWS API calls for their account, including API calls made via the AWS Management Console, the AWS Software Development Kits (SDKs), the command line tools, and higher-level AWS Cloud services. Customers can also identify which users and accounts called AWS APIs for services that support AWS CloudTrail, the source IP address that the calls were made from, and when the calls occurred. Customers can integrate AWS CloudTrail into applications using the API, automate trail creation for their organization, check the status of their trails, and control how administrators turn AWS CloudTrail logging on and off. AWS CloudTrail supports Amazon S3 Data Events. Customers can record all API actions on Amazon S3 objects and receive detailed information.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
Amazon CloudWatch	Amazon CloudWatch is a web service that enables you to collect, view, and analyze metrics. Amazon CloudWatch lets you programmatically retrieve your monitoring data, view graphs, and set alarms to help you troubleshoot, spot trends, and take automated action based on the state of your cloud environment.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price



Service Name	Description	Service Model	Deployment Models	Pricing
AWS Management Console	Access and manage Amazon cloud services through a simple and intuitive web-based user interface. You can also use the AWS Console mobile app to quickly view resources on-the-go.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
AWS Command Line Interface	The AWS Command Line Interface (CLI) is a unified tool used to manage your AWS cloud services. With just one tool to download and configure, you can control multiple AWS cloud services from the command line and automate them through scripts.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
APIs	AWS provides API-based cloud computing services with multiple interfaces to those services, including SDKs, IDE Toolkits, and Command Line Tools for developing and managing AWS resources.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
AWS Elastic Beanstalk	With AWS Elastic Beanstalk, you can quickly deploy and manage applications in the AWS cloud without worrying about the infrastructure that runs those applications. AWS Elastic Beanstalk reduces management complexity without restricting choice or control. You simply upload your application, and AWS Elastic Beanstalk automatically handles the details of capacity provisioning, load balancing, scaling, and application health monitoring.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
AWS CloudFormation	AWS CloudFormation gives developers and system administrators an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion. You can use AWS CloudFormation's sample templates or create your own templates to describe the AWS resources, and any associated dependencies or runtime parameters, required to run your application."	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
AWS CodeDeploy	AWS CodeDeploy is a service that automates code deployments to Amazon EC2 instances. AWS CodeDeploy makes it easier for you to rapidly release new features, helps you avoid downtime during deployment, and handles the complexity of updating your applications. You can use AWS CodeDeploy to automate deployments, eliminating the need for error-prone	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price



Service Name	Description	Service Model	Deployment Models	Pricing
	manual operations, and the service scales with your infrastructure so you can easily deploy to one Amazon EC2 instance or thousands.			
AWS CodeCommit	AWS CodeCommit is a secure, highly scalable, managed source control service that hosts private Git repositories. AWS CodeCommit eliminates the need for you to operate your own source control system or worry about scaling its infrastructure. You can use AWS CodeCommit to store anything from code to binaries, and it supports the standard functionality of Git, allowing it to work seamlessly with your existing Git-based tools.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
AWS CodePipeline	AWS CodePipeline is a continuous delivery and release automation service that aids smooth deployments. You can design your development workflow for checking in code, building the code, deploying your application into staging, testing it, and releasing it to production. You can integrate third-party tools into any step of your release process or you can use AWS CodePipeline as an end-to-end solution.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
AWS OpsWorks	AWS OpsWorks provides a simple and flexible way to create and manage stacks and applications. With AWS OpsWorks, you can provision AWS resources, manage their configuration, deploy applications to those resources, and monitor their health.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
Amazon AppStream	The Amazon AppStream web service deploys your application on AWS infrastructure and streams input and output between your application and devices such as personal computers, tablets, and mobile phones. Your application's processing occurs in the cloud, so it can scale to handle vast computational loads. Devices need only display output and return user input, so the client application on the device can be lightweight in terms of file size and processing requirements.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
Amazon CloudSearch	Amazon CloudSearch is a fully managed service in the cloud that makes it easy to set up, manage, and scale a search solution for your website. Amazon CloudSearch enables you to search large collections of data such as web pages, document	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price



Service Name	Description	Service Model	Deployment Models	Pricing
	files, forum posts, or product information. With Amazon CloudSearch, you can quickly add search capabilities to your website without having to become a search expert or worry about hardware provisioning, setup, and maintenance. As your volume of data and traffic fluctuates, Amazon CloudSearch automatically scales to meet your needs.			
Amazon SWF	Amazon Simple Workflow Service (Amazon SWF) makes it easy to build applications that coordinate work across distributed components. In Amazon SWF, a task represents a logical unit of work that is performed by a component of your application. Coordinating tasks across the application involves managing inter-task dependencies, scheduling, and concurrency in accordance with the logical flow of the application. Amazon SWF gives you full control over implementing tasks and coordinating them without worrying about underlying complexities such as tracking their progress and maintaining their state.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
Amazon Simple Queue Service	Amazon Simple Queue Service (Amazon SQS) is a messaging queue service that handles messages or workflows between other components in a system.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
Amazon SES	Amazon Simple Email Service (Amazon SES) is an outbound-only email-sending service that provides an easy, cost-effective way for you to send email.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
Amazon SNS	Amazon Simple Notification Service (Amazon SNS) is a web service that enables applications, end users, and devices to instantly send and receive notifications from the cloud.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
Amazon Elastic Transcoder	Amazon Elastic Transcoder lets you convert media files that you have stored in Amazon S3 into media files in the formats required by consumer playback devices. For example, you can convert large, high-quality digital media files into formats that users can play back on mobile	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price



Service Name	Description	Service Model	Deployment Models	Pricing
	devices, tablets, web browsers, and connected televisions.			
Amazon Cognito	<p>Amazon Cognito is a simple user identity and data synchronization service that helps you securely manage and synchronize application data for your users across their mobile devices. You can create unique identities for your users through a number of public login providers (Amazon, Facebook, and Google) and support unauthenticated guests.</p> <p>With Amazon CloudSearch, you can quickly add search capabilities to your website without having to become a search expert or worry about hardware provisioning, setup, and maintenance. As your volume of data and traffic fluctuates, Amazon CloudSearch automatically scales to meet your needs.</p>	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
Amazon FPS	Amazon Flexible Payments Service facilitates the digital transfer of money between any two entities, humans or computers.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
AWS Support	AWS Support is a one-on-one, fast-response support channel that is staffed 24x7x365 with experienced and technical support engineers to help customers of all sizes and technical abilities successfully utilize the products and features provided by AWS.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
AWS Trusted Advisor	AWS Trusted Advisor acts like your customized cloud expert, and it helps you provision your resources by following best practices. AWS Trusted Advisor inspects your AWS environment and finds opportunities to save money, improve system performance and reliability, or help close security gaps. Since 2013, customers have viewed over 1.7 million best-practice recommendations, many leading directly to substantial cost reductions.	IaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price

1.4. AWS Marketplace and Related SaaS Offerings

Service Name	Description	Service Model	Deployment Models	Pricing
--------------	-------------	---------------	-------------------	---------



AWS Marketplace	AWS Marketplace is an online store that helps customers find, buy, and immediately start using the software and services they need to build products and run their businesses.	SaaS	All (Public, Private, Hybrid, Community)	Per our AWS reseller agreement, there is no standard discount for Marketplace Offerings.
Amazon WorkDocs	Amazon WorkDocs is a fully managed, secure enterprise storage and sharing service with strong administrative controls and feedback capabilities that improve user productivity. Users can comment on files, send them to others for feedback, and upload new versions without having to resort to emailing multiple versions of their files as attachments.	SaaS	All (Public, Private, Hybrid, Community)	Minimum 2% discount off list price
Amazon Workspaces	Amazon WorkSpaces is a fully managed desktop computing service in the cloud. Amazon WorkSpaces allows customers to easily provision cloud-based desktops that allow end users to access the documents, applications, and resources they need with the device of their choice, including laptops, iPad, Kindle Fire, or Android tablets. With a few clicks in the AWS Management Console, customers can provision a high-quality cloud desktop experience for any number of users at a cost that is highly competitive with traditional desktops and half the cost of most Virtual Desktop Infrastructure (VDI) solutions.	SaaS	All (Public, Private, Hybrid, Community)	Per our AWS reseller agreement, there is no standard discount for Marketplace Offerings.
Splunk Licenses for Logging	As an Elite Splunk Partner, GTRI has the ability to obtain Splunk licenses for a full monitoring platform to be added to any AWS environment.	SaaS	All (Public, Private, Hybrid, Community)	1% off MSRP

1.5. Cloud Solutions Pricing

GTRI offers all AWS IaaS resale offerings at a minimum 2% discount off the AWS list price. This model has several advantages over traditional SKU- based price catalogs:

- **Real Time Discounts.** By providing a discount off list price, we are always able to pass along any price reductions immediately as they occur. This is significant because AWS frequently publishes price reductions and as of 2016 had reduced prices more than 50 times since inception. NASPO ValuePoint Participating Entities get those price reductions immediately without waiting for a formal catalog refresh.



- **Simple and Flexible:** AWS has more than 25,000 SKUs which must be priced individually in a traditional model. We instead use the AWS Calculator to price a complete configuration based on current list price. Our sales engineers can quickly create multiple configurations for comparison based on scenarios and inputs provided by the customer.
- **Transparent:** Customers can always view AWS list pricing in real time. AWS offers a Simple Monthly calculator that is easy to use and includes video tutorials for first-time users. AWS also provides tools that allow customers to evaluate their pricing against other Cloud Service Providers (CSPs).

States may include a wide range of consulting services in their Participating Addendums for all aspects of cloud transition, migration, operations, and optimization.

Rate Card - Hourly

Our hourly ceiling rates for these consulting services are provided below. GTRI does not have different rates for contractor versus customer sites. If necessary, we will negotiate with each purchasing entity for travel costs.

Labor Category	Rate
Enterprise Systems Engineer Level 1	\$117.90
Enterprise Systems Engineer Level 2	\$160.50
Enterprise Systems Engineer Level 3	\$199.80
Enterprise Systems Engineer Level 4	\$239.10
Network Engineer Level 1	\$91.70
Network Engineer Level 2	\$111.35
Network Engineer Level 3	\$147.40
Network Engineer Level 4	\$180.15
Network Engineer Level 5	\$222.70
Wireless Engineer Level 3	\$160.50
Wireless Engineer Level 4	\$186.70
Wireless Engineer Level 5	\$203.05
Project Coordinator Level 1	\$88.45
Project Coordinator Level 2	\$98.25
Project Coordinator Level 3	\$111.35
Project Manager Level 1	\$111.35



Labor Category	Rate
Project Manager Level 2	\$137.55
Project Manager Level 3	\$153.95
Network Security Engineer Level 2	\$117.90
Network Security Engineer Level 3	\$147.40
Network Security Engineer Level 4	\$183.40
Network Security Engineer Level 5	\$203.05
Subject Matter Expert Level 1	\$140.85
Subject Matter Expert Level 2	\$160.50
Subject Matter Expert Level 3	\$199.80
Subject Matter Expert Level 4	\$222.70
Cloud Architect	\$200.16
System Administrator Level 1	\$82.43
System Administrator Level 2	\$100.09
System Administrator Level 3	\$129.52
Cloud Administrator Level 1	\$117.75
Cloud Administrator Level 2	\$141.29
Cloud Administrator Level 3	\$164.84
Splunk Professional Services	\$299.00

PARTICIPATING ADDENDUM EXHIBIT D, INFORMATION TECHNOLOGY PROVISIONS

This Exhibit regarding **Information Technology Provisions** (the "Exhibit") is an essential part of the agreement between the State and Contractor as described in the Contract to which this Exhibit is attached. Unless the context clearly requires a distinction between the Contract and this Exhibit, all references to "Contract" shall include this Exhibit.

4. PROTECTION OF SYSTEM DATA

- A. In addition to the requirements of the main body of this Contract, if Contractor or any Subcontractor is given access to State Records by the State or its agents in connection with Contractor's performance under the Contract, Contractor shall protect all State Records in accordance with this Exhibit. All provisions of this Exhibit that refer to Contractor shall apply equally to any Subcontractor performing work in connection with the Contract.
- B. For the avoidance of doubt, the terms of this Exhibit shall apply to the extent that any of the following statements is true in regard to Contractor access, use, or disclosure of State Records:
 - i. Contractor provides physical or logical storage of State Records;
 - ii. Contractor creates, uses, processes, discloses, transmits, or disposes of State Records;
 - iii. Contractor is otherwise given physical or logical access to State Records in order to perform Contractor's obligations under this Contract.
- C. Contractor shall, and shall cause its Subcontractors, to do all of the following:
 - i. Provide physical and logical protection for all hardware, software, applications, and data that meets or exceeds industry standards and the requirements of this Contract.
 - ii. Maintain network, system, and application security, which includes, but is not limited to, network firewalls, intrusion detection (host and network), annual security testing, and improvements or enhancements consistent with evolving industry standards.
 - iii. Comply with State and federal rules and regulations related to overall security, privacy, confidentiality, integrity, availability, and auditing.
 - iv. Provide that security is not compromised by unauthorized access to workspaces, computers, networks, software, databases, or other physical or electronic environments.
 - v. Promptly report all Incidents, including Incidents that do not result in unauthorized disclosure or loss of data integrity, to a designated representative of the State's Office of Information Security ("OIS").
 - vi. Comply with all rules, policies, procedures, and standards issued by the Governor's Office of Information Technology ("OIT"), including project

lifecycle methodology and governance, technical standards, documentation, and other requirements posted at www.oit.state.co.us/about/policies.

- D. Subject to Contractor's reasonable access security requirements and upon reasonable prior notice, Contractor shall provide the State with scheduled access for the purpose of inspecting and monitoring access and use of State Records, maintaining State systems, and evaluating physical and logical security control effectiveness.
- E. Contractor shall perform current background checks in a form reasonably acceptable to the State on all of its respective employees and agents performing services or having access to State Records provided under this Contract, including any Subcontractors or the employees of Subcontractors. A background check performed within 30 days prior to the date such employee or agent begins performance or obtains access to State Records shall be deemed to be current.
 - i. Contractor will provide notice to the Security and Compliance Representative for the State indicating that background checks have been performed. Such notice will inform the State of any action taken in response to such background checks, including any decisions not to take action in response to negative information revealed by a background check.
 - ii. If Contractor will have access to Federal Tax Information under the Contract, Contractor shall agree to the State's requirements regarding Safeguarding Requirements for Federal Tax Information and shall comply with the background check requirements defined in IRS Publication 1075 and §24-50-1002, C.R.S.

5. DATA HANDLING

- A. The State, in its sole discretion, may securely deliver State Records directly to the facility where such data is used to perform the Work. Contractor may not maintain or forward these State Records to or from any other facility or location, except for the authorized and approved purposes of backup and disaster recovery purposes, without the prior written consent of the State. Contractor may not maintain State Records in any data center or other storage location outside the United States for any purpose without the prior express written consent of OIS.
- B. Contractor shall not allow remote access to State Records from outside the United States, including access by Contractor's employees or agents, without the prior express written consent of OIS. Contractor shall communicate any request regarding non-U.S. access to State Records to the Security and Compliance Representative for the State. The State shall have sole discretion to grant or deny any such request.
- C. Upon request by the State made any time prior to 60 days following the termination of this Contract for any reason, whether or not the Contract is expiring or terminating, Contractor shall make available to the State a complete and secure download file of all data that is encrypted and appropriately authenticated. This download file shall be made available to the State within 10 Business Days of the State's request, and shall contain, without limitation, all State Records, Work Product, and system schema and transformation definitions, or delimited text files with documents, detailed schema definitions along with attachments in its native format. Upon the termination of Contractor's provision of data processing services, Contractor shall, as directed by the State, return all State Records provided by the State to Contractor, and the copies thereof,

to the State or destroy all such State Records and certify to the State that it has done so. If legislation imposed upon Contractor prevents it from returning or destroying all or part of the State Records provided by the State to Contractor, Contractor shall guarantee the confidentiality of all State Records provided by the State to Contractor and will not actively process such data anymore.

- D. The State retains the right to use the established operational services to access and retrieve State Records stored on Contractor's infrastructure at its sole discretion and at any time. Upon request of the State or of the supervisory authority, Contractor shall submit its data processing facilities for an audit of the measures referred to in this Exhibit in accordance with the terms of this Contract.

6. COMPLIANCE

- A. In addition to the compliance obligations imposed by the main body of the Contract, Contractor shall comply with:
- i. All Colorado Office of Information Security (OIS) policies and procedures which OIS has issued pursuant to §§24-37.5-401 through 406, C.R.S. and 8 CCR §1501-5 and posted at <http://oit.state.co.us/ois>
 - ii. All information security and privacy obligations imposed by any federal, state, or local statute or regulation, or by any industry standards or guidelines, as applicable based on the classification of the data relevant to Contractor's performance under the Contract. Such obligations may arise from:
 - a. Health Information Portability and Accountability Act (HIPAA)
 - b. IRS Publication 1075
 - c. Payment Card Industry Data Security Standard (PCI-DSS)
 - d. FBI Criminal Justice Information Service Security Addendum
 - e. CMS Minimum Acceptable Risk Standards for Exchanges
 - f. Electronic Information Exchange Security Requirements and Procedures For State and Local Agencies Exchanging Electronic Information With The Social Security Administration
- B. Contractor shall implement and maintain all appropriate administrative, physical, technical, and procedural safeguards necessary and appropriate to ensure compliance with the standards and guidelines applicable to Contractor's performance under the Contract.
- C. Contractor shall allow the State reasonable access and shall provide the State with information reasonably required to assess Contractor's compliance. Such access and information may include:
- i. The performance of security audit and penetration tests, as requested by OIS or its designee at any time under this Contract;
 - ii. An annual SOC2 Type II audit including, at a minimum, the Trust Principles of Security, Confidentiality, and Availability, or an alternative audit recommended by OIS.

7. INTELLECTUAL PROPERTY ESCROW

- A. Upon request from the State and within the State's sole discretion, Contractor shall deposit the software, documentation, and/or all other related material(s) that are part of the Work with a reputable, State-approved software escrow agent ("Escrow Agent").
- a. For the purposes of this section, software is the source code accompanied by a running object code version submitted on a virus-free magnetic or optical media, compiled and ready to be read by a computer; documentation is all materials sufficient for a trained computer programmer of general proficiency to maintain and support the software without further assistance from Contractor; and all other related material(s) is anything else related to the software or documentation necessary or required for the proper use of the same (such software, documentation and all other related material(s) hereinafter referred to collectively as the "Escrowed Software").
 - b. Contractor shall also have a continuing obligation to deposit any maintenance modifications, updates, upgrades, new releases, or documentation related to the Escrowed Software for the term of the Contract.
- B. Contractor shall enter into an "Escrow Agreement" with the Escrow Agent, which will instruct the Escrow Agent to independently verify the operation of Escrowed Software and cause delivery of the Escrowed Software in Contractor's possession to the State if any one of the following events occurs:
- a. Contractor agrees in writing to the delivery.
 - b. Contractor ceases to do business and the State has not approved a successor to assume Contractor's obligations to the State.
 - c. Contractor has failed to support the Escrowed Software or has otherwise breached this Contract and has exhausted all cure periods to avoid termination for such breach.
 - d. Contractor files for liquidation under the U.S. Bankruptcy Code, or files for reorganization under the U.S. Bankruptcy Code and does not remain debtor in possession.
- C. Contractor shall grant the appropriate license rights in the Escrow Agreement to the Escrow Agent to allow the Escrow Agent to exercise its rights under this Contract. If the Escrow Agent delivers the Escrowed Software to the State, the State shall have the same license and rights to use the Escrowed Software as the State had under this Contract, including, but not limited to, the right to utilize the source code and create updates and derivative works consistent with the purpose of this Contract.
- D. All costs and fees associated with the Escrow Agreement between Contractor and the Escrow Agent for the Escrowed Software shall be the sole responsibility of Contractor. Upon request by the State, Contractor shall provide the State with a copy of the Escrow Agreement.

8. TRANSITION OF SERVICES

Upon expiration or earlier termination of this Contract or any Services provided in this Contract, Contractor shall accomplish a complete transition of the Services from Contractor to the State or any replacement provider designated solely by the State without any interruption of or adverse impact on the Services or any other services provided by third parties in this Contract. Contractor shall cooperate fully with the State or such replacement provider and promptly take all steps required to assist in effecting a

complete transition of the Services designated by the State. All services related to such transition shall be performed at no additional cost beyond what would be paid for the Services in this Contract.

9. LICENSE OR USE AUDIT RIGHTS

- A. Contractor shall have the right, at any time during and throughout the Contract Term, but not more than once per Fiscal Year, to request via written notice in accordance with the notice provisions of the Contract that the State audit its use of and certify as to its compliance with any applicable license or use restrictions and limitations contained in this Contract (an "Audit Request"). The Audit Request shall specify the time period to be covered by the audit, which shall not include any time periods covered by a previous audit. The State shall complete the audit and provide certification of its compliance to Contractor ("Audit Certification") within 120 days following the State's receipt of the Audit Request.
- B. If upon receipt of the State's Audit Certification, the Parties reasonably determine that: (i) the State's use of licenses, use of software, use of programs, or any other use during the audit period exceeded the use restrictions and limitations contained in this Contract ("Overuse") and (ii) the State would have been or is then required to purchase additional maintenance and/or services ("Maintenance"), Contractor shall provide written notice to the State in accordance with the notice provisions of the Contract identifying any Overuse or required Maintenance and request that the State bring its use into compliance with such use restrictions and limitations.

Notwithstanding anything to the contrary in this Contract, or incorporated as a part of Contractor's or any Subcontractor's website, click-through or online agreements, third-party agreements, or any other documents or agreements between the Parties, the State shall not be liable for the costs associated with any Overuse or Maintenance, regardless of whether the State may have been notified in advance of

ATTACHMENT D.1 TO EXHIBIT D – IRS EXHIBIT 7**I. PERFORMANCE**

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

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

II. CRIMINAL/CIVIL SANCTIONS:

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

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

III. INSPECTION:

The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the contractor for inspection of the facilities and operations provided for the performance of any work under this contract. On the basis of such inspection, specific measures may be required in cases where the contractor is found to be noncompliant with contract safeguards.

ATTACHMENT D.2 – HIPAA BUSINESS ASSOCIATE ADDENDUM

This **Exhibit E – HIPAA Business Associate Addendum** (“Addendum”) is part of that certain contract, CMS # _141379 (“Contract”), by and between Zivaro Inc. (“Contractor”) and the State of Colorado (“State”). In the event of a conflict or inconsistency between the Contract and its Exhibits and attachments, such conflict or inconsistency shall be resolved in the manner specified in §8 of the main body of the Contract. Any references to defined terms that are not specifically defined herein shall have the same meaning as those set forth in the Contract and its Exhibits. For purposes of this Addendum, the State is referred to as “Covered Entity” or “CE” and Contractor is referred to as “Associate.” Unless the context clearly requires a distinction between the Contract document and this Addendum, all references herein to “the Contract” or “this Contract” include this Addendum.

RECITALS

- A. CE wishes to disclose certain information to Associate pursuant to the terms of the Contract, some of which may constitute Protected Health Information (“PHI”) (defined below).
- B. CE and Associate intend to protect the privacy and provide for the security of PHI disclosed to Associate pursuant to this Contract in compliance with the Health Insurance Portability and Accountability Act of 1996, 42 USC § 1320d-1320d-8 (“HIPAA”) as amended by the American Recovery and Reinvestment Act of 2009 (“ARRA”)/HITECH Act (PL 111-005), and its implementing regulations promulgated by the US Department of Health and Human Services, 45 CFR Parts 160, 162, and 164 (the “HIPAA Rules”) and other applicable laws, as amended.
- C. As part of the HIPAA Rules, the CE is required to enter into a written contract containing specific requirements with Associate prior to the disclosure of PHI, as set forth in, but not limited to, Title 45, §§ 160.103, 164.502(e), and 164.504(e) of the Code of Federal Regulations (“CFR”) and contained in this Addendum.

The parties agree as follows:

1. Definitions.

- a. Except as otherwise defined herein, capitalized terms in this Addendum shall have the definitions set forth in the HIPAA Rules at 45 CFR Parts 160, 162, and 164, as amended. In the event of any conflict between the mandatory provisions of the HIPAA Rules and the provisions of this Contract, the HIPAA Rules shall control. Where the provisions of this Contract differ from those mandated by the HIPAA Rules, but are nonetheless permitted by the HIPAA Rules, the provisions of this Contract shall control.
- b. “Protected Health Information” or “PHI” means any information, whether oral or recorded in any form or medium: (i) that relates to the past, present, or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under the HIPAA Rules, including, but not limited to, 45 CFR § 164.501.
- c. “Protected Information” shall mean PHI provided by CE to Associate or created, received, maintained, or transmitted by Associate on CE’s behalf. To the extent Associate is a covered entity under HIPAA and creates or obtains its own PHI for treatment, payment, and health care operations, Protected Information under this Contract does not include any

PHI created or obtained by Associate as a covered entity and Associate shall follow its own policies and procedures for accounting, access, and amendment of Associate's PHI.

- d. "Subcontractor" shall mean a third party to whom Associate delegates a function, activity, or service that involves CE's Protected Information, in order to carry out the responsibilities of this Addendum.

2. Obligations of Associate.

- a. Permitted Uses. Associate shall not use Protected Information except for the purpose of performing Associate's obligations under this Contract and as permitted under this Addendum. Further, Associate shall not use Protected Information in any manner that would constitute a violation of the HIPAA Rules if so used by CE, except that Associate may use Protected Information: (i) for the proper management and administration of Associate; (ii) to carry out the legal responsibilities of Associate; or (iii) for Data Aggregation purposes for the Health Care Operations of CE. Additional provisions, if any, governing permitted uses of Protected Information are set forth in **Attachment E.1** to this Addendum. Associate accepts full responsibility for any penalties incurred as a result of Associate's breach of the HIPAA Rules.
- b. Permitted Disclosures. Associate shall not disclose Protected Information in any manner that would constitute a violation of the HIPAA Rules if disclosed by CE, except that Associate may disclose Protected Information: (i) in a manner permitted pursuant to this Contract; (ii) for the proper management and administration of Associate; (iii) as required by law; (iv) for Data Aggregation purposes for the Health Care Operations of CE; or (v) to report violations of law to appropriate federal or state authorities, consistent with 45 CFR § 164.502(j)(1). To the extent that Associate discloses Protected Information to a third-party Subcontractor, Associate must obtain, prior to making any such disclosure: (i) reasonable assurances through execution of a written agreement with such third party that such Protected Information will be held confidential as provided pursuant to this Addendum and only disclosed as required by law or for the purposes for which it was disclosed to such third party; and that such third party will notify Associate within two (2) business days of any breaches of confidentiality of the Protected Information, to the extent it has obtained knowledge of such breach. Additional provisions, if any, governing permitted disclosures of Protected Information are set forth in Attachment A.
- c. Appropriate Safeguards. Associate shall implement appropriate safeguards as are necessary to prevent the use or disclosure of Protected Information other than as permitted by this Contract. Associate shall comply with the requirements of the HIPAA Security Rule at 45 CFR §§ 164.308, 164.310, 164.312, and 164.316. Associate shall maintain a comprehensive written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Associate's operations and the nature and scope of its activities. Associate shall review, modify, and update the documentation of, its safeguards as needed to ensure continued provision of reasonable and appropriate protection of Protected Information.
- d. Reporting of Improper Use or Disclosure. Associate shall report to CE in writing any use or disclosure of Protected Information other than as provided for by this Contract within five (5) business days of becoming aware of such use or disclosure.

- e. Associate's Rights. If Associate uses one or more Subcontractors or agents to provide services under the Contract, and such Subcontractors or agents receive or have access to Protected Information, each Subcontractor or agent shall sign an agreement with Associate containing the same provisions as this Addendum and further identifying CE as a third-party beneficiary with rights of enforcement and indemnification from such Subcontractors or agents in the event of any violation of such Subcontractor or agent agreement. The agreement between Associate and the Subcontractor or agent shall ensure that the Subcontractor or agent agrees to at least the same restrictions and conditions that apply to Associate with respect to such Protected Information. Associate shall implement and maintain sanctions against agents and Subcontractors that violate such restrictions and conditions and shall mitigate the effects of any such violation.
- f. Access to Protected Information. If Associate maintains Protected Information contained within CE's Designated Record Set, Associate shall make Protected Information maintained by Associate or its agents or Subcontractors in such Designated Record Sets available to CE for inspection and copying within ten (10) business days of a request by CE to enable CE to fulfill its obligations to permit individual access to PHI under the HIPAA Rules, including, but not limited to, 45 CFR § 164.524. If such Protected Information is maintained by Associate in an electronic form or format, Associate must make such Protected Information available to CE in a mutually agreed upon electronic form or format.
- g. Amendment of PHI. If Associate maintains Protected Information contained within CE's Designated Record Set, Associate or its agents or Subcontractors shall make such Protected Information available to CE for amendment within ten (10) business days of receipt of a request from CE for an amendment of Protected Information or a record about an individual contained in a Designated Record Set, and shall incorporate any such amendment to enable CE to fulfill its obligations with respect to requests by individuals to amend their PHI under the HIPAA Rules, including, but not limited to, 45 CFR § 164.526. If any individual requests an amendment of Protected Information directly from Associate or its agents or Subcontractors, Associate must notify CE in writing within five (5) business days of receipt of the request. Any denial of amendment of Protected Information maintained by Associate or its agents or Subcontractors shall be the responsibility of CE.
- h. Accounting Rights. If Associate maintains Protected Information contained within CE's Designated Record Set, Associate and its agents or Subcontractors shall make available to CE within ten (10) business days of notice by CE, the information required to provide an accounting of disclosures to enable CE to fulfill its obligations under the HIPAA Rules, including, but not limited to, 45 CFR § 164.528. In the event that the request for an accounting is delivered directly to Associate or its agents or Subcontractors, Associate shall within five (5) business days of the receipt of the request forward it to CE in writing. It shall be CE's responsibility to prepare and deliver any such accounting requested. Associate shall not disclose any Protected Information except as set forth in Section 2(b) of this Addendum.
- i. Governmental Access to Records. Associate shall keep records and make its internal practices, books, and records relating to the use and disclosure of Protected Information available to the Secretary of the US Department of Health and Human Services (the "Secretary"), in a time and manner designated by the Secretary, for purposes of determining CE's or Associate's compliance with the HIPAA Rules. Associate shall

provide to CE a copy of any Protected Information that Associate provides to the Secretary concurrently with providing such Protected Information to the Secretary when the Secretary is investigating CE. Associate shall cooperate with the Secretary if the Secretary undertakes an investigation or compliance review of Associate's policies, procedures, or practices to determine whether Associate is complying with the HIPAA Rules, and permit access by the Secretary during normal business hours to its facilities, books, records, accounts, and other sources of information, including Protected Information, that are pertinent to ascertaining compliance.

- j. Minimum Necessary. Associate (and its agents or subcontractors) shall only request, use, and disclose the minimum amount of Protected Information necessary to accomplish the purpose of the request, use, or disclosure, in accordance with the Minimum Necessary requirements of the HIPAA Rules including, but not limited to 45 CFR §§ 164.502(b) and 164.514(d).
- k. Data Ownership. Associate acknowledges that Associate has no ownership rights with respect to Protected Information.
- l. Retention of Protected Information. Except upon termination of the Contract as provided in Section 4(d) of this Addendum, Associate and its Subcontractors or agents shall retain all Protected Information throughout the term of this Contract and shall continue to maintain the information required under Section 2(h) of this Addendum for a period of six (6) years.
- m. Associate's Insurance. Associate shall maintain insurance to cover loss of PHI data and claims based upon alleged violations of privacy rights through improper use or disclosure of PHI. All such policies shall meet or exceed the minimum insurance requirements of the Contract (e.g. occurrence basis, combined single dollar limits, annual aggregate dollar limits, additional insured status, and notice of cancellation).
- n. Notice of Privacy Practices. Associate shall be responsible for reviewing CE's Notice of Privacy Practices, available on CE's external website, to determine any requirements applicable to Associate per this Contract.
- o. Notification of Breach. During the term of this Contract, Associate shall notify CE within two (2) business days of any suspected or actual breach of security, intrusion, or unauthorized use or disclosure of PHI and/or any actual or suspected use or disclosure of data in violation of any applicable federal or state laws or regulations. Associate shall not initiate notification to affected individuals per the HIPAA Rules without prior notification and approval of CE. Information provided to CE shall include the identification of each individual whose unsecured PHI has been, or is reasonably believed to have been accessed, acquired, or disclosed during the breach. Associate shall take (i) prompt corrective action to cure any such deficiencies and (ii) any action pertaining to such unauthorized disclosure required by applicable federal and state laws and regulations.
- p. Audits, Inspection, and Enforcement. Within ten (10) business days of a written request by CE, Associate and its agents or subcontractors shall allow CE to conduct a reasonable inspection of the facilities, systems, books, records, agreements, policies, and procedures relating to the use or disclosure of Protected Information pursuant to this Addendum for the purpose of determining whether Associate has complied with this Addendum;

provided, however, that: (i) Associate and CE shall mutually agree in advance upon the scope, timing, and location of such an inspection; and (ii) CE shall protect the confidentiality of all confidential and proprietary information of Associate to which CE has access during the course of such inspection. The fact that CE inspects, or fails to inspect, or has the right to inspect, Associate's facilities, systems, books, records, agreements, policies, and procedures does not relieve Associate of its responsibility to comply with this Addendum, nor does CE's (i) failure to detect or (ii) detection, but failure to notify Associate or require Associate's remediation of any unsatisfactory practices, constitute acceptance of such practice or a waiver of CE's enforcement rights under the Contract.

- q. Safeguards During Transmission. Associate shall be responsible for using appropriate safeguards, including encryption of PHI, to maintain and ensure the confidentiality, integrity, and security of Protected Information transmitted pursuant to the Contract, in accordance with the standards and requirements of the HIPPA Rules.
- r. Restrictions and Confidential Communications. Within ten (10) business days of notice by CE of a restriction upon uses or disclosures or request for confidential communications pursuant to 45 CFR § 164.522, Associate will restrict the use or disclosure of an individual's Protected Information. Associate will not respond directly to an individual's requests to restrict the use or disclosure of Protected Information or to send all communication of Protected Information to an alternate address. Associate will refer such requests to the CE so that the CE can coordinate and prepare a timely response to the requesting individual and provide direction to Associate.

3. Obligations of CE.

- a. Safeguards During Transmission. CE shall be responsible for using appropriate safeguards, including encryption of PHI, to maintain and ensure the confidentiality, integrity, and security of Protected Information transmitted pursuant to the Contract, in accordance with the standards and requirements of the HIPAA Rules.
- b. Notice of Changes. CE maintains a copy of its Notice of Privacy Practices on its website. CE shall provide Associate with any changes in, or revocation of, permission to use or disclose Protected Information, to the extent that it may affect Associate's permitted or required uses or disclosures. To the extent that it may affect Associate's permitted use or disclosure of PHI, CE shall notify Associate of any restriction on the use or disclosure of Protected Information that CE has agreed to in accordance with 45 CFR § 164.522.

4. Termination.

- a. Material Breach. In addition to any other provisions on the Contract regarding breach, a breach by Associate of any provision of this Addendum, as determined by CE, shall constitute a material breach of this Contract and shall provide grounds for immediate termination of this Contract by CE pursuant to the provisions of the Contract covering termination for cause, if any. If the Contract contains no express provisions regarding termination for cause, the following terms and conditions shall apply:
 - (1) Default. If Associate refuses or fails to timely perform any of the provisions of this Contract, CE may notify Associate in writing of the non-performance, and if not

promptly corrected within the time specified, CE may terminate this Contract. Associate shall continue performance of this Contract to the extent it is not terminated and shall be liable for excess costs incurred in procuring similar goods or services elsewhere.

- (2) Associate's Duties. Notwithstanding termination of this Contract, and subject to any directions from CE, Associate shall take timely, reasonable, and necessary action to protect and preserve property in the possession of Associate in which CE has an interest.
 - (3) Compensation. Payment for completed supplies delivered and accepted by CE shall be at the Contract Price. In the event of a material breach under paragraph 4a, CE may withhold amounts due Associate as CE deems necessary to protect CE against loss from third-party claims of improper use or disclosure and to reimburse CE for the excess costs incurred in procuring similar goods and services elsewhere.
 - (4) Erroneous Termination for Default. If after such termination it is determined, for any reason, that Associate was not in default, or that Associate's action/inaction was excusable, such termination shall be treated as a termination for convenience, and the rights and obligations of the parties shall be the same as if this Contract had been terminated for convenience, as described in this Contract.
- b. Reasonable Steps to Cure Breach. If CE knows of a pattern of activity or practice of Associate that constitutes a material breach or violation of the Associate's obligations under the provisions of this Addendum or another arrangement and does not terminate this Contract pursuant to Section 4(a), then CE shall take reasonable steps to cure such breach or end such violation. If CE's efforts to cure such breach or end such violation are unsuccessful, CE shall either (i) terminate the Contract, if feasible or (ii) if termination of this Contract is not feasible, CE shall report Associate's breach or violation to the Secretary of the Department of Health and Human Services. If Associate knows of a pattern of activity or practice of a Subcontractor or agent that constitutes a material breach or violation of the Subcontractor's or agent's obligations under the written agreement between Associate and the Subcontractor or agent, Associate shall take reasonable steps to cure such breach or end such violation, if feasible.
- c. Judicial or Administrative Proceedings. Either party may terminate the Contract, effective immediately, if (i) the other party is named as a defendant in a criminal proceeding for a violation of the HIPAA Rules or other security or privacy laws or (ii) a finding or stipulation that the other party has violated any standard or requirement of the HIPAA Rules or other security or privacy laws is made in any administrative or civil proceeding in which the party has been joined.
- d. Effect of Termination.
- (1) Except as provided in paragraph (2) of this subsection, upon termination of this Contract, for any reason, Associate shall return or destroy all Protected Information that Associate or its agents or Subcontractors still maintain in any form, and shall retain no copies of such Protected Information. If associate elects to destroy the PHI, Associate shall certify in writing to CE that such PHI has been destroyed.

- (2) If Associate believes that returning or destroying the Protected Information is not feasible, Associate shall promptly provide CE notice of the conditions making return or destruction infeasible. Associate shall continue to extend the protections of Sections 2(a), 2(b), 2(c), 2(d), and 2(e) of this Addendum to such Protected Information, and shall limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible.

5. Injunctive Relief. CE shall have the right to injunctive and other equitable and legal relief against Associate or any of its Subcontractors or agents in the event of any use or disclosure of Protected Information in violation of this Contract or applicable law.

6. No Waiver of Immunity. No term or condition of this Contract shall be construed or interpreted as a waiver, express or implied, of any of the immunities, rights, benefits, protection, or other provisions of the Colorado Governmental Immunity Act, CRS § 24-10-101 et seq. or the Federal Tort Claims Act, 28 USC § 2671 et seq. as applicable, as now in effect or hereafter amended.

7. Limitation of Liability. Any limitation of Associate's liability in the Contract shall be inapplicable to the terms and conditions of this Addendum.

8. Disclaimer. CE makes no warranty or representation that compliance by Associate with this Contract or the HIPAA Rules will be adequate or satisfactory for Associate's own purposes. Associate is solely responsible for all decisions made by Associate regarding the safeguarding of PHI.

9. Certification. To the extent that CE determines an examination is necessary in order to comply with CE's legal obligations pursuant to the HIPAA Rules relating to certification of its security practices, CE or its authorized agents or contractors may, at CE's expense, examine Associate's facilities, systems, procedures, and records as may be necessary for such agents or contractors to certify to CE the extent to which Associate's security safeguards comply with the HIPAA Rules or this Addendum.

10. Amendment.

- a. Amendment to Comply with Law. The parties acknowledge that state and federal laws relating to data security and privacy are rapidly evolving and that amendment of this Addendum may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of the HIPAA Rules and other applicable laws relating to the confidentiality, integrity, availability, and security of PHI. The parties understand and agree that CE must receive satisfactory written assurance from Associate that Associate will adequately safeguard all Protected Information and that it is Associate's responsibility to receive satisfactory written assurances from Associate's Subcontractors and agents. Upon the request of either party, the other party agrees to promptly enter into negotiations concerning the terms of an amendment to this Addendum embodying written assurances consistent with the standards and requirements of the HIPAA Rules or other applicable laws. CE may terminate this Contract upon thirty (30) days' written notice in the event (i) Associate does not promptly enter into negotiations to amend this Contract when requested by CE pursuant to this Section, or (ii) Associate does not enter into an amendment to this Contract providing assurances regarding the safeguarding of PHI that CE, in its sole discretion, deems sufficient to satisfy the standards and requirements of the HIPAA Rules.

- b. Amendment of Attachment A. Attachment A may be modified or amended by mutual agreement of the parties in writing from time to time without formal amendment of this Addendum.

11. Assistance in Litigation or Administrative Proceedings. Associate shall make itself, and any Subcontractors, employees, or agents assisting Associate in the performance of its obligations under the Contract, available to CE, at no cost to CE up to a maximum of thirty (30) hours, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against CE, its directors, officers, or employees based upon a claimed violation of the HIPAA Rules or other laws relating to security and privacy or PHI, except where Associate or its Subcontractor, employee, or agent is a named adverse party.

12. No Third-Party Beneficiaries. Nothing express or implied in this Contract is intended to confer, nor shall anything herein confer, upon any person other than CE, Associate, and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

13. Interpretation and Order of Precedence. The provisions of this Addendum shall prevail over any provisions in the Contract that may conflict or appear inconsistent with any provision in this Addendum. Together, the Contract and this Addendum shall be interpreted as broadly as necessary to implement and comply with the HIPAA Rules. The parties agree that any ambiguity in this Contract shall be resolved in favor of a meaning that complies and is consistent with the HIPAA Rules. This Contract supersedes and replaces any previous separately executed HIPAA addendum between the parties.

14. Survival of Certain Contract Terms. Notwithstanding anything herein to the contrary, Associate's obligations under Section 4(d) ("Effect of Termination") and Section 12 ("No Third-Party Beneficiaries") shall survive termination of this Contract and shall be enforceable by CE as provided herein in the event of such failure to perform or comply by the Associate. This Addendum shall remain in effect during the term of the Contract including any extensions.

15. Representatives and Notice.

- a. Representatives. For the purpose of the Contract, the individuals identified elsewhere in this Contract shall be the representatives of the respective parties. If no representatives are identified in the Contract, the individuals listed below are hereby designated as the parties' respective representatives for purposes of this Contract. Either party may from time to time designate in writing new or substitute representatives.
- b. Notices. All required notices shall be in writing and shall be hand delivered or given by certified or registered mail to the representatives at the addresses set forth below.

State/Covered Entity Representative

Name: _____
 Title: _____
 Department and Division: _____
 Address: _____

Contractor/Business Associate Representative

Name: Todd Olson

Title: VP Sales

Department and Division: Sales

Address: Zivaro, Inc.

990 S. Broadway, Suite 300

Denver, CO 80209

720-836-7387

contracts@zivaro.com

ATTACHMENT D.3 – HIPAA BAA ATTACHMENT

This **Attachment E.1 – HIPAA BAA Attachment** is part of that certain contract, CMS # 139963 (“Contract”), by and between Zivaro Inc. (“Contractor”) and the State of Colorado acting by and through the Governor’s Office of Information Technology (“State” or “OIT”). In the event of a conflict or inconsistency between the Contract and its Exhibits and attachments, such conflict or inconsistency shall be resolved in the manner specified in §8 of the main body of the Contract. Any references to defined terms that are not specifically defined herein shall have the same meaning as those set forth in the Contract and its Exhibits.

This Attachment sets forth additional terms to the HIPAA Business Associate Addendum, which is part of the Contract, and is effective as of the Effective Date of the Contract (the “Attachment Effective Date”). This Attachment may be amended from time to time as provided in § 10(b) of the Addendum.

16. Additional Permitted Uses. In addition to those purposes set forth in § 2(a) of the Addendum, Associate may use Protected Information as follows: _____

17. Additional Permitted Disclosures. In addition to those purposes set forth in § 2(b) of the Addendum, Associate may disclose Protected Information as follows: _____

18. Subcontractor(s). The parties acknowledge that the following subcontractors or agents of Associate shall receive Protected Information in the course of assisting Associate in the performance of its obligations under this Contract: _____

19. Receipt. Associate’s receipt of Protected Information pursuant to this Contract shall be deemed to occur as follows, and Associate’s obligations under the Addendum shall commence with respect to such PHI upon such receipt: _____

20. Additional Restrictions on Use of Data. CE is a Business Associate of certain other Covered Entities and, pursuant to such obligations of CE, Associate shall comply with the following restrictions on the use and disclosure of Protected Information: _____

21. Additional Terms. *[This section may include specifications for disclosure format, method of transmission, use of an intermediary, use of digital signatures or PKI, authentication, additional security of privacy specifications, de-identification or re-identification of data and other additional terms.]* _____
