A G R E E M E N T

THIS AGREEMENT ("Agreement") is made between the **CITY AND COUNTY OF DENVER**, a municipal corporation of the State of Colorado (the "City") and Ventiv Technology, Inc., a California Corporation registered to do business in Colorado, whose address is 3350 Riverwood Parkway, Suite 2000, Atlanta, GA 30339 ("Contractor"), jointly "the parties."

IT IS HEREBY AGREED BETWEEN THE PARTIES AS FOLLOWS:

1. **DEFINITIONS**. Whenever used herein, any schedules, exhibits, or addenda to this Agreement, the following terms shall have the meanings assigned below. Other capitalized terms used in this Agreement are defined in the context in which they are used.

1.1 ***"Affiliate"*** means any entity that controls, is controlled by, or is under common control with Contractor. For purposes of the Agreement, "control" means possessing, (i) directly or indirectly, the power to direct or cause the direction of the management, policies or operations of an entity, whether through ownership of voting securities, by contract or otherwise; or (ii) the ownership of, or the power to vote, at least fifty percent (50%) of the voting stock, shares or interests of such entity.

1.2 ***"Agreement"*** means this Cloud Computing Services Agreement between City and Contractor, inclusive of all schedules, exhibits, attachments, addenda and other documents incorporated by reference between the City and Contractor, Contract Number 201846023.

1.3 ***"Business Day"*** collectively means Monday through Friday of each week, other than days on which banks in Marietta, Georgia, U.S.A, are closed for banking and any other date designated by Contractor as a holiday to City from time-to-time as such in advance in writing (because different holidays may be recognized on different days each year);

1.4 **"*Change Request*"** has the meaning set forth in Section 15.2;

1.5 ***"Brand Features"*** means the trade names, trademarks, service marks, logos, domain names, and other distinctive brand features of each party, respectively, as secured by such party from time to time.

1.6 ***"City Data"*** includes credentials issued to City by Contractor and all records relating to City's use of Contractor Services and administration of End User accounts, including any Protected Information of City personnel that does not otherwise constitute Protected Information of an End User.

1.7 ***"Confidential Information"*** means any Data that a disclosing party treats (1) in a confidential manner and that is (2) marked "Confidential Information" or is considered "Protected Information" prior to disclosure to the other party. 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 ***"Data"*** means all information, whether in oral or written (including electronic) form, created by or in any way originating with City and End Users, 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 City and End Users, in the course of using and configuring the Services provided under this Agreement, and includes City Data, End User Data, and Protected Information.

1.9 **"*City Support Services*"** has the meaning set forth in Section 8.1(d);

1.10 ***"Data Compromise"*** means any actual or reasonably suspected unauthorized access to or acquisition of computerized Data that compromises the security, confidentiality, or integrity of the Data, or the ability of City to access the Data.

1.11 **"*Deliverables*"** means those Services detailed in the Statement of Work to be performed during implementation of the System to enable Production Use of the System, including without limitation, (i) Project Management – managing the project delivery; (ii) Business Analysis – requirements gathering, specifications, QA testing; (iii) Configuration – setup of City database including custom fields and custom business rules; (iv) Data Conversion – convert source data into format used by the Software; (v) Reporting – deploy standard templates, complete custom report development, as applicable, (vi) Training – training for City testing and go-live;

1.12 **"*Derivative Works*"** means any suggestions, contributions, enhancements, improvements, modifications or changes to the referenced materials;

1.13 ***"Documentation"*** means, collectively: (a) all materials published or otherwise made available to 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 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 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 City.

1.14 ***"Downtime"*** means any period of time of any duration that the Services are not made available by Contractor to City for any reason, including scheduled maintenance or Enhancements.

1.15 ***"End User"*** means the individuals (including, but not limited to employees, authorized agents, students and volunteers of City; Third Party consultants, auditors and other independent contractors performing services for City; any governmental, accrediting or regulatory bodies lawfully requesting or requiring access to any Services; customers of City provided services; and any external users collaborating with City) authorized by City to access and use the Services provided by Contractor under this Agreement.

1.16 ***"End User Data"*** includes End User account credentials and information, and all records sent, received, or created by or for End Users, including email content, headers, and attachments, and any Protected Information of any End User or third party contained therein or in any logs or other records of Contractor reflecting End User's use of Contractor Services.

1.17 ***"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 the Contractor has elected to make generally available to its customers.

1.18 ***"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.

1.19 ***"Protected Information"*** includes but is not limited to personally-identifiable information, student records, protected health information, criminal justice information or individual financial information (collectively, "Protected Information") that is subject to local, state or federal statute, regulatory oversight or industry standard restricting the use and disclosure of such information and that the loss of such Protected Information would constitute a direct damage. These include, but are not limited to: the Colorado Constitution, the Colorado Consumer Protection Act, the Children's Online Privacy Protection Act (COPPA), Health Insurance Portability and Accountability Act (HIPAA), the Family Education Rights and Privacy Act (FERPA), the Payment Card Industry Data Security Standard (PCI DSS), and the Federal Bureau of Information Criminal Justice Information Services (CJIS) Security Policy.

1.20 **"*Production Use*"** means the capability to use, or the actual use of, the Software and System in a live environment;

1.21 **"*Project*"** means the scope of work to be performed by Contractor as set forth in the Statement of Work;

1.22 ***"Project Manager"*** means the individual who shall serve as each party's point of contact with the other party's personnel as provided in this Agreement. The initial Project Managers and their contact information are set forth in the Notices section below and may be changed by a party at any time upon written notice to the other party.

1.23 **"*Project Plan*"** means the methodology for completing the Project to be agreed by the parties at the initial requirements meeting following execution of the Agreement;

1.24 ***"RFP Response"*** means any proposal submitted by Contractor to City in response to City's Request for Proposal ("RFP") titled Risk Management Information System 28659Q and issued May 18, 2018.

1.25 ***"Service"*** means Contractor's computing solutions, provided to 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.

1.26 "***Software***" means the object code to Contractor's proprietary software products listed in Exhibit A, and any modified, updated or enhanced versions of, or additional modules related to, such software products that Contractor provides to City either pursuant to the maintenance and support provisions or pursuant to an

SOW, as well as the Software Configurations and the Documentation for such software products, including any Derivative Works of such software and documentation;

1.27 "***Software Configurations***" means any of the Deliverables set forth in the SOW related to configuration or modification of the Software or of the standard reports or templates within the Software or the creation of business rules using the Software;

1.28 "***Software Customizations***" means any customizations to the Software requested by City that requires changes to the actual source code of the Software or creation of a completely new interface.

1.29 "***Specifications***" means the software specifications set forth in the Documentation and in the Statement of Work for the relevant Software product;

1.30 **"*Statement of Work*"** or **"*SOW*"** means the statement of work set forth in Attachment 1 to this Agreement as well as any changes or amendment to such SOW or any new SOWs that may be attached to a new SOW; and

1.31 **"*System*"** is the collective reference to the Software, Software Configurations, Documentation, Contractor Server, and other technology that together comprises the hosted system offered to City under this Agreement.

1.32 ***"Third Party"*** means persons, corporations and entities other than Contractor, City or any of their employees, contractors or agents.

1.33 ***"Third Party Host"*** means that the servers where the Contractor's software resides is at physical location which is not controlled by the Contractor, sometimes called "managed hosting", for example, Amazon Web Service.

1.34 **"*Contractor Content*"** means any information, data, materials, software, files, text, graphics, photographs, audio visual elements, music, illustrations, video or other content available through the System which is proprietary to Contractor, its licensors, or Contractor's affiliates;

1.35 **"*Contractor Server*"** means those computer servers that Contractor owns, leases or otherwise controls whether in its own data center or the data center of another entity with which Contractor has a contractual relationship;

2. RIGHTS AND LICENSE IN AND TO DATA

2.1 City is the sole and exclusive owner of all City Data and all Intellectual Property Rights in the foregoing, whether or not provided to any other party under this Agreement. City Data will be governed under this section of the Agreement. Contractor will not use City Data for any purpose other than that of providing the Software or rendering the Services under this Agreement, nor sell, assign, lease, or dispose of City Data. City assumes full responsibility for its employees, vendors, representatives, agents, and its clients ("City Representatives") with respect to the transmission of City Data sent directly by City to Contractor. City must ensure that all City Representatives provide such City Data to Contractor via either an encryption process or a secure transport mechanism. City assumes full responsibility to safeguard against unauthorized access and provide appropriate protection of its City Data prior to and during the transmission or transfer of its City Data to Contractor. City and Contractor acknowledge that the accuracy of delivering the Software and Services depends upon the accuracy and completeness of the City Data and/or business requirements needed to deliver the Software and

Services by Contractor. City accepts sole responsibility for errors in the Software or Services to the extent resulting from inaccurate or incomplete City Data supplied to Contractor by City or City Representatives. Contractor has the right to use the City Data for benchmarking purposes provided that Contractor completely de-identifies all such City Data. All End User Data and City Data created and/or processed by the Services is and shall remain the property of City and shall in no way become attached to the Services, nor shall Contractor have any rights in or to the Data of City.

2.2 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.

2.3 City retains the right to use the Services to access and retrieve City Data stored on Contractor's Services infrastructure at any time during the term at its sole discretion.

3. DATA PRIVACY

3.1 Contractor will use City Data and End User Data only for the purpose of fulfilling its duties under this Agreement and for City's and its End User's sole benefit and will not share such Data with or disclose it to any Third Party without the prior written consent of City or as otherwise required by law. By way of illustration and not of limitation, Contractor will not use such Data for Contractor's own benefit and, in particular, will not engage in "data mining" of Data or communications, whether through automated or human means, except as specifically and expressly required by law or authorized in writing by City.

3.2 Contractor will provide access to Data only to those Contractor employees, contractors and subcontractors ("Contractor Staff") who need to access the Data to fulfill Contractor's obligations under this Agreement. Contractor will ensure that, prior to being granted access to the 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 the Data they will be handling.

4. DATA SECURITY AND INTEGRITY

4.1 In the event that the Service is provided with a Third-Party Host, Contractor shall not be relieved of the obligations in Sections 4, 6, 7 and 8, under this Agreement.

4.2 Contractor uses a layered approach to information security. Contractor will use commercially reasonable efforts to maintain the security, integrity and availability of all City Data to which it has access, including but not limited to commercially reasonable efforts reflecting changing technological approaches, to comply with the following measures: (a) HIPPA Security Rule; (b) ISO 27001; (c) maintain a documented Information Security Program which includes annual risk assessment and management procedures; (d) maintain the principle of least privilege; (e) classify and handle all City data as confidential and apply the necessary security

and controls to support HIPAA/HITECH Act compliance; (f) maintain commercially customary physical security and access controls for its data center(s); (g) maintain commercially customary network security controls including firewall and intrusion prevention solutions; (h) maintain commercially customary redundancy at the demark, network and system layers; (i) maintain commercially customary monitoring solutions to continually manage health and capacity of the IT infrastructure components; (j) provide data encryption in a commercially customary manner of all data transmissions; (k) require a minimum of 128-bit SSL encryption for application access and use; (l) maintain and update anti-virus program; (m) require individual user accounts and passwords for any access; (n) maintain strong password requirements for all Contractor-managed accounts; (o) maintain generally acceptable user account management processes and procedures; (p) maintain industry accepted data protection program; (q) maintain whole disk encryption for all laptops; (r) deploy software security patches in accordance with generally accepted industry best practices; (s) maintain and periodically test (at least annually) a commercially customary disaster recovery plan that provides adequate system backup, technology replacement, and alternate (backup-site) site capabilities; (t) follow commercially customary hardening procedures for system/device builds; (u) conduct ongoing vulnerability management through the use of commercially customary tools; (v) conduct periodic (at least annually) third party vulnerability assessments; (w) follow Open Web Application Security Project (OWASP) methodologies, guidelines and techniques for application development; (x) follow commercially customary change and release management practices for hardware and software changes; (y) follow commercially customary asset sanitization procedures to ensure decommissioned equipment is free of any and all City Data; (z) maintain City Data security using commercially customary database and application controls; (aa) notify City of any unauthorized access to City Data immediately upon discovery; and (bb) maintain at least one certification or attestation covered in Section 7.3 above or replacement standard on security practices from a nationally or globally recognized provider of such reports. Contractor warrants that all City Data and End User Data will be encrypted in transmission (including via web interface) and in storage

4.3 Contractor shall at all times 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.

4.4 Prior to the Effective Date of this Agreement, Contractor or Third-Party Host, will at its expense conduct or have conducted the following, and thereafter, Contractor, or Third-Party Host, will at their expense conduct or have conducted the following at least once per year, and immediately after any actual or reasonably suspected Data Compromise of City Data:

4.4.1 A SSAE 18/SOC 1 Type 2 or industry equivalent audit of Contractor's security policies, procedures and controls;

4.4.2 A quarterly external and internal vulnerability scan, performed by a City-approved Third-Party scanner, of Contractor's systems and facilities 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;

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

4.5 Contractor will provide 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.

4.6 If any critical or high deficiencies are identified based on the results and recommendations of the above audits, certifications, scans and tests, Contractor will, within sixty (60) calendar days of receipt of such results, promptly modify its security measures in order to meet its obligations under this Agreement and provide City with written evidence of remediation.

4.7 Contractor shall protect Data against deterioration or degradation of Data quality and authenticity.

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 Data, Contractor will notify City in writing immediately upon receiving notice of such requirement and prior to any such disclosure;

5.1.2 Consult with City regarding its response;

5.1.3 Cooperate with 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 City's request, provide City with a copy of its response.

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

6. DATA COMPROMISE RESPONSE

6.1 Contractor shall report, either orally or in writing, to City any Data Compromise involving Data, or circumstances that could have resulted in unauthorized access to or disclosure or use of Data, not authorized by this Agreement or in writing by City, including any reasonable belief that an unauthorized individual has accessed Data. Contractor shall make the report to City immediately upon discovery of the unauthorized disclosure, but in no event more than two (2) business after Contractor reasonably believes there has been such unauthorized use or disclosure. Oral reports by Contractor regarding Data Compromises will be reduced to writing and supplied to City as soon as reasonably practicable, but in no event more than forty-eight (48) hours after oral report.

6.2 Immediately upon becoming aware of any such Data Compromise, Contractor shall fully investigate the circumstances, extent and causes of the Data Compromise, and report the results to City and continue to keep City informed on a daily basis of the progress of its investigation until the issue has been effectively resolved.

6.3 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.

6.4 Within five (5) calendar days of the date Contractor becomes aware of any such Data Compromise, Contractor shall have completed implementation of corrective actions to remedy the Data Compromise, restore City access to the Services as directed by City, and prevent further similar unauthorized use or disclosure.

6.5 Contractor, at its expense, shall cooperate fully with City's investigation of and response to any such Data Compromise incident if compromise is Contractor's fault.

6.6 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 City.

6.7 Notwithstanding any other provision of this Agreement, and in addition to any other remedies available to City under law or equity, and where the Contractor was at fault for the compromise, Contractor will promptly reimburse City in full for all costs incurred by City in any investigation, remediation or litigation resulting from any such Data Compromise, 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 Compromise in such a fashion that, in 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 Compromise.

6.8 The preceding requirements of this Section 6 are applicable to the Contractor and the Service to the extent the Contractor maintains control over the Service and the software and the requirements are not in violation of the agreement between the Contractor and the Third-Party Host.

7. DATA RETENTION AND DISPOSAL

7.1 Contractor will retain Data in a City's account, including attachments, until the City deletes them or for the time period mutually agreed to by the parties in this Agreement.

7.2 Using appropriate and reliable storage media, Contractor will regularly backup Data.

7.3 At the City's election, Contractor will either securely destroy or transmit to City repository any backup copies of City Data. Contractor will supply City a certificate indicating the records disposed of, the date disposed of, and the method of disposition used.

7.4 Contractor will retain logs associated with End User activity consistent with industry best practices and any specific regulatory requirements.

7.5 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

City indicating that those records may be relevant to litigation that City reasonably anticipates. Oral requests by 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. 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 City.

8. DATA TRANSFER UPON TERMINATION OR EXPIRATION

8.1 Upon termination or expiration of this Agreement, Contractor will ensure that all Data are securely transferred to City, or a Third Party designated by City, within thirty (30) calendar days. Contractor will ensure that such migration uses facilities and methods that are compatible with the relevant systems of City, and that City will have access to Data during the transition. In the event that it is not possible to transfer the aforementioned data to City in a format that does not require proprietary software to access the data, Contractor shall provide City with an unlimited use, perpetual license to any proprietary software necessary in order to gain access to the Data.

8.2 Contractor will provide City with no less than ninety (90) calendar days' notice of impending cessation of its business. This includes immediate transfer of any previously escrowed assets and Data.

8.3 Along with the notice described above, Contractor will provide a fully documented service description and perform and document a gap analysis by examining any differences between its Services and those to be provided by its successor.

8.4 Contractor will provide a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to City.

8.5 Contractor shall implement its contingency and/or exit plans and take all necessary actions to provide for an effective and efficient transition of service with minimal disruption to City. Contractor will work closely with its successor to ensure a successful transition to the new service and/or equipment, with minimal Downtime and effect on City, all such work to be coordinated and performed no less than ninety (90) calendar days in advance of the formal, final transition date.

9. **SERVICE LEVELS**. Incorporated into Agreement and Scope of Work.

10. **INTERRUPTIONS IN SERVICE; SUSPENSION AND TERMINATION OF SERVICE; CHANGES TO SERVICE**. Incorporated into Agreement and Scope of Work.

11. **INSTITUTIONAL BRANDING.** Contractor Services will provide reasonable and appropriate opportunities for City branding of Contractor Services. Each party shall have the right to use the other party's Brand Features only in connection with performing the functions provided in this Agreement and as specified in the attached Plan. Any use of a party's Brand Features will inure to the benefit of the party holding Intellectual Property Rights in and to those features. Contractor may not advertise that City is a client, list City as a reference or otherwise use City's name, logos, trademarks, or service marks without prior written permission obtained from City personnel authorized to permit City brand use.

12. **COMPLIANCE WITH APPLICABLE LAWS AND CITY POLICIES.** Contractor will comply with all applicable laws in performing Services under this Agreement. Any Contractor personnel visiting City's facilities will comply with all applicable City policies regarding access to, use of, and conduct within such facilities. City will provide copies of such policies to Contractor upon request.

13. WARRANTIES, REPRESENTATIONS AND COVENANTS

13.1 Services Warranty. For sixty (60) days after the performance of any Services under this Agreement, Contractor warrants that such Services will be performed in a professional and workmanlike manner consistent with generally accepted industry practices. For any breach of this services warranty, City's exclusive remedy, and Contractor's entire liability, will be the re-performance of such deficient Contractor Services. City must identify in a written notice to Contractor any deficiencies in such Services within ninety (90) days of completion of such deficient Services in order to receive the above warranty remedies.

13.2 **Software Warranty.** Following Production Use of the System, Contractor represents and warrants that during the Term the System will perform substantially in accordance with the Specifications for the System. If Contractor receives written notice that the System does not perform as warranted within sixty (60) days of such non-performance, Contractor will, at its option and at no additional charge to City, undertake to correct errors, or replace such portions of the System free of charge with software that performs as warranted hereunder. If Contractor is unable to repair or replace the non-conforming software, then City's sole and exclusive remedy against Contractor will be to terminate this Agreement and receive a pro-rata refund of annual License Fees paid under the Agreement for its use of the System for the terminated portion of the Term. For the avoidance of doubt, Contractor will not be responsible for payment of any fines assessed against City by any regulatory authority for failure of the City to comply with statutory or regulatory requirements of any kind which are not the fault of Contractor.

13.3 **City Warranty.** City represents and warrants that City is authorized to provide Contractor with the City Data and that Contractor is authorized to use such City Data solely for the purpose of providing the System and Services.

13.4 **Exclusions.** Contractor does not warrant and is not responsible for (a) any third-party products not provided by Contractor, or (b) services not provided solely by Contractor, its agents and subcontractors.

13.6 **DISCLAIMER.** OTHER THAN AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER CONTRACTOR, ITS AFFILIATES, LICENSORS OR SUPPLIERS, NOR THEIR OFFICERS, DIRECTORS, EMPLOYEES, SHAREHOLDERS, AGENTS OR REPRESENTATIVES MAKES ANY EXPRESS OR IMPLIED WARRANTIES, CONDITIONS, OR REPRESENTATIONS TO CUSTOMER, OR ANY OTHER PERSON OR ENTITY WITH RESPECT TO THE SOFTWARE, SYSTEM AND SERVICES PROVIDED HEREUNDER OR OTHERWISE REGARDING THIS AGREEMENT, WHETHER ORAL OR WRITTEN, EXPRESS, IMPLIED OR STATUTORY, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, THE IMPLIED WARRANTY

AGAINST INFRINGEMENT, AND THE IMPLIED WARRANTY OR CONDITION OF FITNESS FOR A PARTICULAR PURPOSE. CONTRACTOR DOES NOT WARRANT THAT THE OPERATION OF THE SOFTWARE, SYSTEM OR SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE. Warranty of Authority. Each party represents and warrants that it has the right to enter into this Agreement. Contractor represents and warrants that it has the unrestricted right to provide the Services, and that it has the financial viability to fulfill its obligations under this Agreement. Contractor represents, warrants and agrees that the Services shall be free and clear of all liens, claims, encumbrances or demands of third parties. Contractor represents and warrants that it has no knowledge of any pending or threatened litigation, dispute or controversy arising from or related to the Services. This warranty shall survive the expiration or termination of this Agreement

14. CONFIDENTIALITY

14.1 Each party acknowledges that certain information that it shall acquire from the other is of a special and unique character and constitutes Confidential Information.

14.2 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 either party 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 City are potentially subject to applicable state and federal law, including the Colorado Open Records Act, and that the release of Confidential Information required by applicable law will not constitute a breach or threatened breach of this Agreement.

14.3 Except as expressly provided by the terms of this Agreement, each party agrees that it shall not disseminate, transmit, license, sublicense, assign, lease, release, publish, post on the internet, transfer, sell, permit access to, distribute, allow interactive rights to, or otherwise make available any data, including Confidential Information or any part thereof to any other person, party or entity in any form of media for any purpose other than performing its obligations under this Agreement. Contractor further acknowledges that by providing Data or Confidential Information, the City is not granting to Contractor any right or license to use such data except as provided in this Agreement. Contractor further agrees not to disclose or distribute to any other party, in whole or in part, the Data or confidential information without written authorization from the Manager and will immediately notify the City if any information of the City is requested from the Contractor from a Third Party.

14.4 Each party agrees, with respect to the Confidential Information, that: (1) either

party shall not copy, recreate, reverse engineer or decompile such Data or Confidential Information, in whole or in part, unless authorized in writing by the other party; (2) either party shall retain no copies, recreations, compilations, or decompilations, in whole or in part, of such Data or Confidential Information; and (3) Contractor shall, upon the expiration or earlier termination of the Agreement, destroy (and, in writing, certify destruction) or return all such Data or Confidential Information or work products incorporating such Data or Confidential Information to the City. Each party will inform its employees and officers of the obligations under this Agreement, and all requirements and obligations of the parties under this Agreement shall survive the expiration or earlier termination of this Agreement. Neither party shall disclose 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.

14.5 Notwithstanding any other provision of this Agreement, the City is furnishing Data or Confidential Information on an "as is" basis, without any support whatsoever, and without representation, warranty or guarantee, including but not in any manner limited to, fitness, merchantability or the accuracy and completeness of the Data or Confidential Information. Contractor is hereby advised to verify its work.

15. <u>PROTECTED INFORMATION.</u> During the course of this Agreement, should Contractor come into possession of any Protected Information, Contractor shall take all commercially necessary steps to protect the information from release and otherwise conform to the requirements of the BAA, attached.

16. <u>SOFTWARE AS A SERVICE, SUPPORT AND SERVICES TO BE PERFORMED:</u>

16.1 Subject to payment by City of the Fees detailed in the Exhibit A, Contractor, under the general direction of, and in coordination with, the Director of Risk Management or other designated supervisory personnel (the "Manager") agrees to provide the Services listed on Exhibits A and B and perform the technology related services described on attached Exhibits A and B (the "Statement of Work" or "SOW"). Contractor has the sole right and obligation to supervise, manage, contract, direct, procure, perform, or cause to be performed the Services to be performed by Contractor hereunder unless otherwise provided herein. Contractor may, as it deems appropriate, use subcontractors for all or any portion of the Services. Contractor may at any time remove and replace any such subcontractors.

16.1.1 Implementation Services. Contractor will provide the implementation services described in the Statement of Work ("Implementation Services").

16.1.2 Training Services. Contractor will provide the training services to City described in the SOW ("Training Services").

16.1.3 Hosting Services. Contractor will host the Software on Contractor's Servers to provide the System to City in accordance with the terms of this Agreement, which will include administration of database objects, table structure, table space, scheduled programs, stored procedures, and automated backup and recovery processes performed by Contractor to the Software ("Hosting Services").

16.1.4 Support and Maintenance Services. Contractor will provide the customer

support and maintenance services described herein ("City Support Services").

16.1.5 Transitional Services. At City's expense on a time-and-materials basis, (which shall not exceed $220 an hour during the term of this Agreement) Contractor will provide City with reasonable assistance in the winding down of the Services and/or transition of such Services to a new service provider in the event of any termination or expiration of this Agreement.

16.2 As the Manager directs, the Contractor shall diligently undertake, perform, and complete all of the technology related services and produce all the deliverables set forth on Exhibit B to the City's satisfaction.

16.3 The Contractor is ready, willing, and able to provide the technology related services and the Services required by this Agreement.

16.4 The 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.

16.5 Change Control Procedures. Either party may during the implementation of the Project (as detailed in the SOW) request a change to any aspect of the Project Plan ("Change Request"). Such Change Request is to be delivered by the requesting party's Project manager (a "Project Manager") to the other party's Project Manager. For the avoidance of doubt, any redefinition of the scope of services by City, or the provision by City of new details in respect of the implementation, will be deemed to constitute a Change Request. A Change Request must contain a detailed and complete explanation of the proposed changes. If there is any dispute as to whether a change requested by City is within or beyond the scope of the Project Plan, Contractor will not be obliged to proceed with that change until that dispute is resolved and will proceed in accordance with the Project Plan as it then exists. If a Change Request is executed by authorized signatories of both parties, Contractor will perform the services detailed in the Change Request in accordance with the terms and conditions of this Agreement (subject to any specific terms of the Change Request itself), and such executed Change Request will constitute an amendment to this Agreement and the applicable Statement of Work.

16.6 City Obligations. City will maintain a designated representative who will be authorized to act as the primary point of contact for Contractor in dealing with City with respect to each party's obligations under this Agreement and on a timely basis and at no charge to Contractor, issue all consents or approvals and make all requests on behalf of City. City will establish and maintain, at its own expense, all telecommunications equipment and access lines necessary to gain access to and support transmission of the Software via the System. City agrees to perform all tasks assigned to City as set forth in this Agreement, the SOW, or any Project Plan or as reasonably requested by Contractor and provide all assistance and cooperation to Contractor in order to accomplish timely and efficiently the Services. Contractor will not be deemed in breach of this Agreement or SOW in the event Contractor's failure to meet the responsibilities and time schedules set forth in the SOW or any Project Plan is caused by City's failure to meet (or delay in) its responsibilities and time schedules set forth in the applicable SOW, this Agreement or as otherwise requested by Contractor. In the event of any delay in City's performance of any of

the obligations set forth in this Agreement, including any Statement of Work, or any other delays caused by City, the milestones, fees and date(s) set forth in the Statement of Work or Project Plan will be adjusted as reasonably necessary to account for such delays.

16.7 Additional Services. In the future, City may purchase additional services by executing an SOW describing the proposed services and fee payment schedule. A new Statement of Work describing in detail the services to be provided may be attached to such SOW (a "New Statement of Work"). Once the New Statement of Work are signed by both parties it will be incorporated herein by reference and made a part of this Agreement. No New Statement of Work will become effective until it has been executed by an authorized representative of both Contractor and City and attached to an SOW. Any services detailed in a New Statement of Work will be deemed to be "Services" under this Agreement.

16.8 Excluded Services. To the extent City requires any Software Customizations, the services required to provide such Software Customizations will be subject to a separately executed professional services agreement between the parties.

16.9 City Support, Hosting and SLAs.

16.9.1 City Support Services. Contractor will provide the City Support Services set forth in Schedule C. The initial term for the City Support Services will be as set forth in the SOW in Exhibit B ("Initial Maintenance Term").

16.10 Hosting and SLAs. Contractor will host the System in accordance with the service levels set forth in Schedule C. The initial term for the Hosting Services will be as set forth in the SOW in Exhibit B ("Initial Hosting Term").

17. PASSWORDS.

17.1 City's Obligations. City will be given all applicable passwords to use in connection with the System and will ensure that each user is given their own individual user ID and password, which may not be shared with another individual for any reason. City will be responsible for changing such passwords immediately upon first use of the System. City is entirely responsible for maintaining the confidentiality of such passwords and of its accounts (including, if applicable, the passwords and accounts of each of the City personnel accessing the System by means of an account established by City). City is responsible for all access to and use of the System through City's passwords.

17.2 Unauthorized Access**.** Contractor is not responsible for any unauthorized access and/or use by any third party who independently gains access to City's instance of the Software on the System and/or related information, provided that such access is not caused or contributed to by Contractor. City will notify Contractor promptly of any unauthorized use of any user accounts or of any other breach of security occurring as a result of any activities of any of City's end-users or of any vulnerabilities that City believes are contained in or caused by the System such that Contractor may take or recommend appropriate remedial measures. Contractor will have no liability for any loss of Protected Information or damage arising from City's failure to comply with the provisions of this Agreement.

17.3 Contractor and City agree (a) to maintain and update an industry standard anti-virus program within their respective computer systems and (b) to use commercially reasonable efforts to check attachments to e-mail messages that a party receives

before saving such attachments to their respective organization's hard drives or servers.

17.4 **Vendor Supported Releases**. The Contractor, at its sole discretion, shall maintain the appropriate currency for all third-party software used in the development and execution or use of the software 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.

17.5 **Oracle 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.

18. GRANT OF LICENSE; RESTRICTIONS:

18.1 Access License. Subject to the terms and conditions of this Agreement, including, but not limited to, payment by City of the applicable fees set forth on the SOW, Contractor grants to City a limited, non-exclusive, non-transferable (except as permitted hereunder) license, without the right to sublicense (except as permitted under Section 17.2 below), to remotely access and use the System that is located on the Contractor Server in accordance with the terms of this Agreement for the length of the Hosting Term (as defined hereunder). Use of the System is limited to employees of City for whom Contractor has received notification and those parties specifically authorized in Section 17.2 below, such notification provided when requesting passwords for such users. Contractor authorizes City to use, copy and distribute Contractor Content provided that (1) the use and distribution of Contractor Content is limited to City, its representatives, and/or its clients, and (2) all copies of Contractor Content will retain all copyright or proprietary notices. Any other use or distribution of Contractor Content, unless authorized in writing by Contractor, is prohibited. The license granted under this Section 18.1 is referred to as the "Access License."

18.2 Other Authorized Users.

18.2.1 Third-Party Vendors. Contractor acknowledges and agrees that City may use certain third-party vendors for purposes of performing some of City's internal business processes ("Third-Party Vendors"). City may allow its Third-Party Vendors (other than Contractor's direct competitors) to access and use the System subject to the terms and conditions of this Agreement solely for City's internal business processing services, subject to the following conditions: (i) City agrees to be fully responsible for all use of the System by its Third-Party Vendors; (ii) City will ensure compliance by Third-Party Vendors of the terms and conditions of this Agreement, including without limitation, Section 14 of this Agreement (Confidential Information); (iii) City will notify Contractor of any such Third-Party

Vendors (such notification provided when requesting passwords for such Third Party Vendors) and will ensure that each such Third-Party Vendor uses its own unique password as detailed in Section 16 below; and (iv) upon termination of its relationship with such Third-Party Vendors or of this Agreement, City will ensure that all access to the System by such Third-Party Vendors ceases immediately.

18.3 Limitations

18.3.1 Use Restrictions. Unless otherwise expressly authorized in this Agreement, City will not, and will ensure that its end-users will not: (i) modify, adapt, alter, translate, or create derivative works from the System; (ii) merge the Software or System (or any part thereof) with any other software, products or services (other than Contractor-provided interfaces); (iii) sublicense, resell, re-distribute, lease, rent, loan, disclose or otherwise transfer the Software or System (or any part thereof) or any other associated products and services to any third party; (iv) reverse engineer, decompile, disassemble, or otherwise attempt to derive the source or object code of the Software or System (or any part thereof); (v) use the Software or System (or any part thereof) to provide any facility management, service bureau or similar services to third parties, permit third parties to remotely access and use the Software or System (or any part thereof) or use the Software or System (or any part thereof) to develop a product line that is similar to the Software or Software or System; (vi) publish or share with any third party any results of any benchmark or performance tests run on the Software or System (or any part thereof); (vii) otherwise use or copy the Software or System (or any part thereof) except as expressly allowed under this Agreement or (viii) alter, distort, or remove any confidential, proprietary, copyright, trademark, trade secret, or patent legends from any copy of the Software or System (or any part thereof).

18.3.2 Unauthorized Actions. In addition, City agrees that it will not use the Software or System to take any action that: (i) violates any applicable law or regulation or is legally libelous, defamatory, indecent, obscene or pornographic; (ii) would violate copyright, trademark, trade secret or other property right of any third party; (iii) involves the addition, removal or modification of identifying network header information in an effort to deceive; (iv) uses the System to access, or attempt to access, the accounts of others, or to penetrate, or attempt to penetrate, security measures of Contractor's or another entity's computer software or hardware, electronic communications system, or telecommunications system, whether or not the intrusion results in access to or the corruption or loss of data; (vi) uses the Software or System to collect, or attempt to collect, personal information about third parties without their valid consent.

18.3.3 Removal of Files. Contractor reserves the right to remove from the Contractor Server(s) any files that may damage the System or any files that are in violation of this Section, provided that Contractor agrees to give City written notice within two (2) Business Days after removing such files. The removed files will be placed in a temporary quarantined area until both parties mutually agree how to handle the files. City consents to such removal and waives any claim arising out of any such file removal.

18.3.4 Additional Software. To the extent City wishes to purchase additional Contractor software products other than that set forth in Exhibit A, City and Contractor will execute an order form to purchase such additional software.

18.3.5 Proprietary Rights. As between the parties, and subject to the terms and conditions of this Agreement and the applicable Statement of Work, Contractor and its third-party suppliers will retain ownership of all Intellectual Property Rights in the System, and any and all Derivative Works made to the System or any part thereof, as well as all Work Product provided to City ("Contractor Proprietary Technology"). City acquires no rights to Contractor Proprietary Technology except for the licensed interests granted under this Agreement or any SOW. The term "Work Product" means all other materials, reports, manuals, visual aids, documentation, ideas, concepts, techniques, inventions, processes, or works of authorship developed, provided or created by Contractor or its employees or contractors during the course of performing work for City (excluding any City Data or Derivative Works thereof and excluding any output from the System generated by City's use of the System, including without limitation, reports, graphs, charts, modified City Data, etc., but expressly including any form templates of such reports, graphs or charts by themselves that do not include City Data). City also acknowledges that the Contractor Proprietary Technology contains Confidential Information belonging to Contractor and its third-party suppliers, and that nothing herein gives City any right, title or interest in such Contractor Proprietary Technology except as otherwise expressly set forth in this Agreement or in any SOW. City acknowledges and agrees that Contractor may use, without restriction, all suggestions, improvements and ideas concerning any part of the System (including without limitation any Beta Versions as defined herein) or Intellectual Property Rights therein that may be communicated to Contractor by City. City agrees to inform Contractor immediately of any infringement or other improper action with respect to Contractor's Confidential Information, the System or the Intellectual Property Rights therein that comes to City's attention.

18.3.6 Rights Reserved. Title, ownership rights, and all Intellectual Property Rights in and to the System will remain the sole property of Contractor or its suppliers. City acknowledges that the Software in source code form remains Confidential Information or a trade secret of Contractor and/or its suppliers, that the source code is not covered by any license hereunder and will not be provided by Contractor. Except as set forth in this Agreement, no right or implied license or right of any kind is granted to City, regarding the System or any part thereof. Nothing in this Agreement confers upon either party any right to use the other party's trade names and trademarks, except for permitted license use in accordance with this Agreement. All use of such marks by either party will inure to the benefit of the owner of such marks, use of which will be subject to specifications controlled by the owner.

19. <u>DELIVERY AND ACCEPTANCE:</u>

19.1 During the implementation of the Service, the City may test and evaluate same to ensure that it conforms, upon mutual agreement between Contractor and City, to the specifications outlined in the SOW or the Documentation. If at any time any warranted portion of the Service does not conform to the Specifications provided in Exhibit C, the City will notify Contractor in writing within sixty (60) days and City and Contractor will mutually agree to a solution, to repair or replace the nonconforming product in an agreed upon time frame, at Contractor's expense if the portion of the service that is nonconforming is warranted pursuant to this Agreement. The foregoing procedure will be repeated until the City accepts or finally rejects the product, 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. In the event that 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.

19.2 If the City is not satisfied with the Contractor's performance of the technology related services described in the SOW, the City will so notify Contractor within thirty (30) days after Contractor's performance thereof. Contractor will, re-perform the service per Exhibit C 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. In the event that City finally rejects any technology related service, Contractor will refund to City all fees paid by City with respect to such technology related service.

20. **TERM**: The term of the Agreement is from December 1, 2018 through December 31, 2023. The Effective Date of the Agreement is below on the Signature page.

21. COMPENSATION AND PAYMENT:

21.1 Fee: The fee for the Service and technology related services is described in Exhibits A and B (the "Fee"). The Fee shall be paid pursuant to the City's Prompt Payment Ordinance.

21.2 Reimbursement Expenses: The fees specified above include all expenses, and no other expenses shall be separately reimbursed hereunder. Notwithstanding the foregoing, Travel and Travel expenses will be pre-approved by City and billed as incurred.

21.3 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.

21.4 Maximum Contract Liability:

21.4.1 Notwithstanding any other provision of the Agreement, the City's maximum payment obligation will not exceed **ONE MILLION T WO HUNDRED THOUSAND DOLLARS** ($1,200,000.00) (the "Maximum Contract 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 Exhibits A and B. Any services performed
beyond those in Exhibits A and B are performed at Contractor's risk and without authorization under the Agreement.

21.4.2. 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.

22. **STATUS OF CONTRACTOR:** The Contractor is an independent contractor retained to perform professional or technical services for limited periods of time. Neither the 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.

23. TERMINATION:

23.1 Termination for Breach. In the event that either party materially defaults in the performance of any of its duties or obligations under this Agreement and does not substantially cure such default, or commence a cure, within thirty (30) days after being given written notice specifying the default, the non-defaulting party may, by giving written notice thereof to the defaulting party, terminate this Agreement. Contractor may, by written notice to City, terminate City's right to use the System without liability to City, if City fails to pay the applicable fees for the System as set forth in the SOW within thirty (30) days after Contractor gives City notice of such nonpayment. Any such suspension or termination of access to the System does not relieve City from paying any past due amounts and any amounts due Contractor through the expiration date of this Agreement.

23.2 Termination for Convenience. The City has the right to terminate the Agreement with cause upon written notice effective immediately, and without cause upon one hundred-eighty (180) days prior written notice to the Contractor. However, nothing gives the Contractor the right to perform services under the Agreement beyond the time when its services become unsatisfactory to the Manager. The foregoing notwithstanding, if City terminates this Agreement at any time following the sixth (6^{th}) month of the Term but prior to the conclusion of the Term for reasons other than Breach, City shall be obligated to pay the following: (a) in year one of the Agreement, $400,000; (b) in year two of the Agreement $300,000; (c) in year three of the Agreement, $ $200,000; (d) in year four of the Agreement, $100,000. Upon any Termination for Convenience, the City shall be obligated to pay any charges accrued but unpaid as of the termination date.

23.3 Effect of Termination. Within thirty (30) days (or earlier upon Contractor's reasonable written request) after the effective date of a termination of this Agreement for any reason, City will (i) pay Contractor for all services performed by Contractor up to the effective date of such termination and all other amounts owed by City to Contractor under this Agreement including, but not limited to, all Fees, which shall not include any kind of services not received by the City, that are owed

by City as of the effective date of termination according to the payment schedule set forth in the SOW, regardless of the date of termination; and (ii) destroy or return to Contractor all Contractor property, including, but not limited to all Documentation and the Confidential Information of Contractor. Upon the destruction or return of such materials, City will provide Contractor with a signed written statement certifying that it has destroyed or returned all Contractor property to Contractor. Upon termination of this Agreement for any reason, all rights and licenses granted by Contractor hereunder to City will immediately cease.

23.4 Return of City Data. When requested in writing by City, based upon termination of the Access License, Contractor will deliver (within sixty (60) days of receipt of request) electronic files containing all available City Data. Contractor will deliver the data files in a normalized, ASCII, flat file format. The files will be encrypted and posted to an agreed to SFTP site. Standardized documentation describing the data files will be included. All work completed by Contractor for the extract of the data will be billed to the City on a time and materials basis. Sixty (60) days following termination of the Access License, all City Data in the System will no longer be available on Contractor's Systems, as Contractor will purge all such City Data from its Systems, and all such City Data will either be returned to City if requested in accordance with this Section 22.4 or, if return of data is not requested, it will be destroyed, unless otherwise agreed by the parties in writing. All data received from third parties for City will also be deleted from Contractor's Systems within the 60-day period.

23.5 Survival. Termination of this Agreement will not affect survival of the provisions regarding Contractor's or City's treatment of Confidential Information, provisions relating to the payments of amounts due that have accrued prior to termination, indemnity provisions, provisions limiting or disclaiming the party's liability, or the provisions on termination, which provisions will survive such termination.

23.6 Notwithstanding the preceding paragraph, the City may terminate the Agreement if the 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.

23.7 Upon termination of the Agreement, with or without cause, the 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.

24. **EXAMINATION OF RECORDS:** 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 any pertinent books, documents, papers and records of the Contractor, involving transactions related to the Agreement until the latter of three (3) years after the final payment under the Agreement or expiration of the applicable statute of limitations.

25. **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.

26. INSURANCE:

26.1 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, or any extension thereof, during any warranty period, and for three (3) years after termination of the Agreement. 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 contain a valid provision or endorsement requiring notification to the City in the event any of the required policies is 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. If any policy is in excess of a deductible or self-insured retention, the City must be notified by the Contractor. 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.

26.2 Proof of Insurance: Contractor shall provide a copy of this Agreement to its insurance agent or broker. Contractor may not commence services or work relating to the Agreement prior to placement of coverages required under this Agreement. Contractor certifies that the certificate of insurance attached as Exhibit C, preferably an ACORD certificate, complies with all insurance requirements of this Agreement. The City requests that the City's contract number be referenced on the Certificate. 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.

26.3 Subcontractors and Subconsultants: All subcontractors and subconsultants (including independent contractors, suppliers or other entities providing goods or services required by this Agreement) shall be subject to all of the requirements herein and shall procure and maintain the same coverages required of the Contractor. Contractor shall include all such subcontractors as additional insured under its policies (with the exception of Workers' Compensation) or shall ensure that all such subcontractors and subconsultants maintain the required coverages. Contractor agrees to provide proof of insurance for all such subcontractors and subconsultants upon request by the City.

26.4 Workers' Compensation/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. Contractor expressly represents to the City, as a material representation upon which the City is relying in entering into this Agreement, that none of the Contractor's officers or employees who may be eligible under any statute or law to reject Workers' Compensation Insurance shall effect such rejection during any part of the term of this Agreement, and that any such rejections previously effected, have been revoked as of the date Contractor executes this Agreement.

26.5 Commercial General Liability: Contractor shall maintain a Commercial General Liability insurance policy with limits of $1,000,000 for each occurrence, $1,000,000 for each personal and advertising injury claim, $2,000,000 products and completed operations aggregate, and $2,000,000 policy aggregate.

26.6 Professional or Errors & Omissions: Contractor shall maintain Professional or Errors and Omissions insurance including cyber liability, network security, privacy liability and product failure coverage with limits of $1,000,000 per occurrence and $1,000,000 policy aggregate.

26.7 Additional Provisions:

26.7.1 For Commercial General Liability, the policy must provide the following:

26.7.1.1 That this Agreement is an Insured Contract under the policy;

26.7.1.2 Defense costs are outside the limits of liability;

26.7.1.3 A severability of interests or separation of insureds provision (no insured vs. insured exclusion); and

26.7.1.4 A provision that coverage is primary and non-contributory with other coverage or self-insurance maintained by the City.

26.7.2 For claims-made coverage:

26.7.2.1 The retroactive date must be on or before the contract date or the first date when any goods or services were provided to the City, whichever is earlier

26.7.2.2 Contractor shall advise the City in the event any general aggregate or other aggregate limits are reduced below the required per occurrence limits. At their own expense, and where such general aggregate or other aggregate limits have been reduced below the required per occurrence limit, the Contractor will procure such per occurrence limits and furnish a new certificate of insurance showing such coverage is in force.

27. **REPRESENTATION AND WARRANTY:** Contractor represents and warrants that:

27.1 The Service will conform to applicable specifications, operate in substantial compliance with applicable Documentation, and will be free from deficiencies and defects in materials, workmanship, design and/or performance;

27.2 all technology related services will be performed by qualified personnel in a professional and workmanlike manner, consistent with industry standards;

27.3 all technology related services will conform to applicable specifications and the Exhibits attached hereto;

27.4 it 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 any and all liens, adverse claims, encumbrances and interests of any Third Party;

27.5 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;

27.6 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;

27.7 the software and Service will contain no malicious or disabling code that is intended to damage, destroy or destructively alter software, hardware, systems or data.

28. DEFENSE AND INDEMNIFICATION:

28.1 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.

28.2 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.

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

28.4 Contractor will indemnify, defend, and hold City, its individual directors, officers, employees and agents, harmless from and against any claims, actions or proceedings, arising out of any third-party claim (a) that the Software or the permitted use thereof infringes or violates any third party's valid U.S. patent, copyright or trade secret ("IP Claim"); or (b) arising from Contractor's or Contractor's employees' or subcontractors' gross negligence or intentional misconduct in the performance of the Services under this Agreement. If in Contractor's reasonable judgment any such IP Claims, or threat of an IP Claim, materially interferes with City's use of the Software, Contractor will consult with City, and Contractor will have the option, in Contractor's sole discretion, to (i) substitute functionally equivalent non-infringing software or documentation, (ii) modify the Software to make it non infringing, (iii) obtain for City at Contractor's expense the right to continue using the infringing Software; or, if the foregoing is not feasible in Contractor's sole discretion, Contractor will (iv) require City to cease using the System, refund a pro-rata portion of the annual License Fees (as defined in the SOW) for the System for such period of time in which City was unable to use the Software or System. Contractor will have no indemnity obligation for claims of infringement resulting or alleged to result from (i) any combination, operation, or use of any Software with any programs or equipment not supplied by Contractor or not specified in this Agreement for such purpose if in Contractor's reasonable judgment such infringement would have been avoided by the combination, operation, or use of such Software with items supplied by Contractor or specified in this Agreement for such purpose; (ii) inclusion of City Data; (iii) any modification of the Software by a party other than Contractor if such infringement would have been avoided in the absence of such modifications; or (iv) the use of the Software in a manner other than for its intended purposes or contrary to the Specifications. This Section 28.4 states Contractor's entire liability and City's sole and exclusive remedy for infringement claims and actions.

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

28.6 General. The defense and indemnification obligations set forth in this Section 28

are conditioned upon (i) the indemnified party providing the indemnifying party timely notice of any claim or cause of action upon which the indemnified party intends to base a claim of indemnification hereunder, (ii) the indemnified party providing reasonable assistance and cooperation to enable the indemnifying party to defend the action or claim hereunder; and (iii) allowing the indemnifying party to control the defense and all related settlement negotiations subject to the City's approval; provided that the indemnifying party may not settle any claim that results in the indemnified party's liability and the indemnifying party will be required to consult with the indemnified party during any settlement discussions and receive approval from the City.

28.7 **LIMITATION OF LIABILITY**.

28.7.1 LIMITATION OF REMEDY. EXCEPT AS PROHIBITED BY LAW, IN NO EVENT WILL EITHER PARTY, OR ITS CONTRACTORS, LICENSORS OR SUPPLIERS OR ANY OF THEIR OFFICERS, DIRECTORS, EMPLOYEES, SHAREHOLDERS, AGENTS OR REPRESENTATIVES BE LIABLE TO THE OTHER PARTY, OR ANY OTHER PERSON OR ENTITY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, INDIRECT, EXEMPLARY, OR PUNITIVE DAMAGES OR LIABILITIES FOR ANY CAUSE WHATSOEVER ARISING OUT OF OR RELATING TO THIS AGREEMENT, INCLUDING ALL STATEMENTS OF WORK, ORDER FORMS, OR AMENDMENTS THERETO, WHETHER IN CONTRACT OR TORT OR OTHERWISE, INCLUDING A BREACH THEREOF OR INCLUDING DAMAGES OR LIABILITIES FOR LOST PROFIT, LOST REVENUE, LOSS OF USE, LOSS OF GOODWILL, LOSS OF REPUTATION, THE COST OF ANY SUBSTITUTE EQUIPMENT, SOFTWARE PROGRAM, REGARDLESS OF WHETHER THE POSSIBILITY OF SUCH DAMAGES OR LIABILITIES HAVE BEEN COMMUNICATED TO SUCH PARTY AND REGARDLESS OF WHETHER SUCH PARTY HAS OR GAINS KNOWLEDGE OF THE EXISTENCE OF SUCH DAMAGES OR LIABILITIES. LOSS OF PERSONAL HEALTH INFORMATION IS A DIRECT DAMAGE.

28.7.2 EXCEPT FOR (I) CLAIMS FOR INFRINGEMENT BY THE CONTRACTOR, (II) THE RECOVERY OF SUMS DUE UNDER THIS AGREEMENT OR IN AN SOW; OR (III) AS PROHIBITED BY LAW, IN NO EVENT WILL CONTRACTOR'S LIABILITY FOR DAMAGES TO CITY, REGARDLESS OF THE FORM OF ACTION, WHETHER BASED ON CONTRACTOR, TORT, NEGLIGENCE, STRICT LIABILITY, PRODUCTS LIABILITY, OR OTHERWISE, EVER EXCEED $3,600,000. NOTWITHSTANDING THE FORGOING, CONTRACTOR'S MAXIMUM LIABILITY FOR ANY CLAIM INVOLVING DATA BREACH OR LOSS OF PERSONAL HEALTH INFORMATION EVER EXCEED $7,000,000.

29. **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).

30. **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.

31. **ASSIGNMENT; SUBCONTRACTING:** Except as otherwise set forth in this Agreement, this Agreement and all rights and obligations may not be assigned (by operation of law or otherwise) in whole or in part by City, and any such attempted assignment will be void and of no effect; provided, however, that either party hereto will have the right to assign this Agreement to another entity in connection with a reorganization, merger, consolidation, acquisition or other restructuring involving all or substantially all of the voting securities and/or assets of the assigning party upon written notice to the non-assigning party.

32. **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 the Contractor receiving services or benefits pursuant to the Agreement is an incidental beneficiary only.

33. **NO AUTHORITY TO BIND CITY TO CONTRACTS:** The 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.

34. **AGREEMENT AS COMPLETE INTEGRATION-AMENDMENTS:** 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.

35. **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.

36. CONFLICT OF INTEREST:

36.1 No employee of the City shall have any personal or beneficial interest in the services or property described in the Agreement. The 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.

36.2 The Contractor shall not engage in any transaction, activity or conduct that would result in a conflict of interest under the Agreement. The 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 the Contractor by placing the Contractor's own interests, or the interests of any party with whom the 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 the Contractor written notice describing the conflict.

37. **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:

Director of Risk Management or Designee
201 West Colfax Avenue, Dept. 1105
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.

38. **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.

39. **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.

40. **NO DISCRIMINATION IN EMPLOYMENT:** In connection with the performance of work under this contract, the Contractor may not refuse to hire, discharge, promote or demote, or discriminate in matters of compensation against any person otherwise qualified, solely because of race, color, religion, national origin, gender, age, military status, sexual orientation, gender identity or gender expression, marital status, or physical or mental disability. The Contractor shall insert the foregoing provision in all subcontracts.

41. **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.

42. **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.

43. **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.

44. **ORDER OF PRECEDENCE:** In the event of any conflicts between the language of the Agreement and the exhibits, the language of the Agreement controls.

45. **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, the 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.

46. **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.

47. **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.

48. **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.

49. **PARAGRAPH HEADINGS:** The captions and headings set forth herein are for convenience of reference only and shall not be construed so as to define or limit the terms and provisions hereof.

50. **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.

51. **COUNTERPARTS OF THIS AGREEMENT:** This Agreement may be executed in counterparts, each of which shall be deemed to be an original of this Agreement.

52. **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.

53. **ADVERTISING AND PUBLIC DISCLOSURE:** The Contractor shall not include any reference to the Agreement or to services performed pursuant to the Agreement in any of the 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. The 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.

54. **COMPLIANCE FOR IN-SCOPE SERVICES.** The Contractor covenants and agrees to comply with the processing, handling, and security standards and guidelines as set forth by, but not limited to:

    a) Health Insurance Portability and Accountability Act (HIPAA)
    b) Family Education Rights and Privacy Act (FERPA)
    c) Children's Online Privacy and Protection Act (COPPA)

d) Federal Bureau of Investigation Criminal Justice Information Systems (CJIS) Security Policy

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 Data under this Agreement maintain compliance with and comply in full of 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 Data may be utilized within the Services that change the compliance requirements. In the event that compliance requirements change, the Contractor and City shall collaborate in good faith and use all reasonable efforts to become or remain compliant as necessary under this section. In the event that compliance is required or statutory and no reasonable efforts are available, the City at its discretion may terminate the agreement for cause.

55. **ON-LINE AGREEMENT DISCLAIMER.** Any 'click-wrap' agreement, terms of use, electronic acceptance or other terms and conditions which attempt to govern the subject matter of this Agreement that either party might be required to acknowledge or accept before or after entering into this Agreement are of no force and effect as between the City and Contractor and are superseded by this Agreement.

ATTACHED EXHIBITS

EXHIBIT A-SOFTWARE DESCRIPTION, ORDER FORM, SUPPORT & HOSTING SERVICE LEVELS SCHEDULE
EXHIBIT B-STATEMENT OF WORK
EXHIBIT C-CERTIFICATE OF INSURANCE
EXHIBIT D-BAA

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

Contract Control Number:

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:

By_____

By_____

By_____

Contract Control Number: FINAN-201846023-00

Contractor Name: VENTIV TECHNOLOGY INC

By: _____

Name: DAVID J. EVANS
(please print)

Title: SENIOR CORPORATE COUNSEL
(please print)

ATTEST: [if required]

By: _____

Name: Natalia Rodriguez
(please print)

Title: Billing Supervisor
(please print)

EXHIBIT A

Schedule A to the iVOS Software License & Support Agreement

Software Description

The Software being provided to Customer are the iVOS and Risk Console Advance® products that include a number of different modules. Part I below includes a description of each module within the Software that the Customer will have a right to use based on the Fees set forth in the Order Form. Part II below describes the different user types and the level of access granted to each type of user. The Order Form will designate what type of users the Customer has purchased.

I. iVOS

A. Claim Administration Modules

1. **Workers' Compensation Module**
   iVOS automatically calculates all temporary disability (TD) and permanent disability (PD) rates, given an incident date and a wage information. Additionally, the system can be set up to schedule and generate TD payments automatically. Other key worker's compensation features of iVOS include:
   - Jurisdiction-specific forms and letters for all 50 states
   - OSHA 300, 301, 300A tracking and report generation
   - Work status tracking
   - Multiple dependent tracking
   - Calculation of most jurisdictional standard compensation rates
   - Medical management
   - Business rules to facilitate compliance with state requirements
   - Option to produce the Employer's First Report of Injury (FROI) and/or Subsequent Report of Injury (SROI)

2. **Property and Casualty Module**
   For processing of Property and Casualty claims, such as General Liability, Professional Liability, Automobile Insurance, and other such Property and Casualty Lines of Business. The iVOS Property & Casualty module is specifically designed to support multiple claimants to one incident. Each claimant supports its own set of financials and ancillary information (diary, notepad, correspondence, email, etc.). However, reports and online viewing of financial reserve information can be rolled up to the occurrence level. Other iVOS liability claim features include:
   - Tracking of multiple claimants per incident as well as initial claimant demand and multi-vehicle information
   - Contact management
   - Multiple employer tracking
   - Vehicle reporting
   - Traffic-accident tracking

Core Components Included. Each of the core components listed below comes standard with either of the modules listed above under Claims Administration Modules.

- Business Rules – iVOS includes a full business rules engine with hundreds of rule templates that can be used to manage workflow for claims, including monitoring (e.g., notifying supervisors of open claims with no diary activity in X days) and event-driven rules (e.g., sending forms/letters for new claims). As Customer creates its own business rules, it can name each rule as desired, and even create its own folder system for organizing the rules. Existing rules can be moved or copied from folder to folder as needed, making it easy to create new rules that are similar to an existing rule.

- Workflow Queues – iVOS has the capability to define workflow queues

- Searches - All claims can be looked up through the query functionality on the iVOS home page. For example, on the home page, Claimant Search tab can find claims based on one or more of the following criteria: Claim Number, Social Security Number, Insured, Adjusting Office, Injured Part, Claimant Liability, Employee Number, Policy, Examiner, Medical Record Number, Incident From and Through Dates, Insurer Name, Affiliate Claim Number, and Insurance Type. Search results can be managed easily in iVOS through multi-tiered sorting and filtering capabilities (which can be set as user preferences to apply to future searches), as well as the ability to "lock" selected columns for easy visual reference while scrolling through results. iVOS also includes auto-complete and extended search (e.g., vendor and contact records in addition to claims) options to help users find the records they want.

- Diary Management –. Each user can track their diary activities in iVOS. Diaries can be manually entered or generated automatically by business rules. These activities can be filtered by category, priority, and date range to help manage an examiner's caseload. User may also view diary activities at a claim level, showing all diaries scheduled for a single claim, enabling multiple users to collaborate on a claim. Security can be applied to diaries, restricting access by a combination of confidentiality level and diary category types, enabling certain groups of users to have diaries that cannot be seen by other workgroups. In addition, iVOS gives users the ability to temporarily re-assign diaries for examiners who are on leave, or simply to oversee an examiner's workload to make sure he or she is not getting behind or "stair stepping" their diaries.

- Notepads - Used for documenting conversations, creating action plans, attaching electronic files such as photographs, and more. iVOS provides unlimited free-form text entry in the notepad body that can be manually or automatically spell-checked upon saving (using American, legal, and medical dictionaries). Each notepad category can have a customizable template associated with it, enabling customers to establish standards for data capture in the notepad. In addition, security can be applied to specific notepad types (for example, case manager notes that can be hidden from examiners). Similarly, users can use a filtering option to view only notepads that meet selected criteria.

- Correspondence - iVOS integrates with Microsoft Word for managing written correspondence, using user-definable templates stored in the application server. Users can generate a letter from a claim file simply by selecting a master group from a drop-down list, then choosing a specific letter within that group from another drop-down list. iVOS then merges data from the claim file into the letter based on the template, and displays the letter in Microsoft Word on the user's computer for any additional editing and/or formatting. When custom changes to the letter are complete, the user will have a choice of saving the letter in draft mode or final mode (final mode will disallow further changes to the letter). Sent correspondence is can be locked in the database as read only, but can be easily retrieved and viewed. Other features of iVOS correspondence include:
  - Inserting an examiner's signature
  - Customized form/letter headers and footers
  - Prompts for selection certain fields such as care providers, legal counsel, payment amounts, etc., associated with the claim in forms that require an objective decision
  - Auto-calculated fields such as benefit totals.
  - CA EAMS Forms – eForms option – The CA Division of Workers' Compensation, Electronic Adjudication Management System forms **(**EAMS forms) are provided and maintained within iVOS. iVOS supports the eForms solution option**. JET filing is not supported at this time**

- Payments and Reserves - iVOS financial functionality is broken into two main areas, payments and reserves. Both functional areas are governed by business rules, SIR limits established by the policies, and user payment and reserve authority limits. iVOS allows users to create "unapproved" payments and reserves above their authority limits. When "unapproved" payments or reserves are created, supervisors can be notified in real time through their User Diary, or these transactions can be queued in a list for a supervisor to review periodically through the day, approving them in bulk or individually. Payments that are due, but have unapproved reserves, unapproved payments, incomplete addresses, etc., will not be authorized for printing, but will be caught on a payment report specifying the reason for not being authorized (which can be distributed for correction). iVOS also has the ability to schedule a series of payments that auto-calculate the benefit to be paid over a period of weeks, and schedule the payments for release on their proper due date.

- Vendor Management - iVOS provides vendor management capabilities, including vendor search options from the home page and the payment screen (for selecting a vendor to pay). The Vendor Payment record has fields for tracking a vendor's name, address, main contact, vendor type and specialty, and ACH information for electronic funds transfer. In addition, iVOS allows you to combine payments from multiple claims onto one vendor payment, as well as to have multiple vendor locations with a single tax ID. Other features include managing withholding payments for multiple date periods, W9 form requests, and other correspondence to the vendor. iVOS also has a built-in interface that ensures compliance with federal Office of Foreign Assets Control (OFAC) regulations during the vendor payment process by performing a search against OFAC's published list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries.

- Policy Maintenance Module - iVOS provides comprehensive insurer, bank account, insured, policy, policy period, reinsurance, and agent tracking for policy verification, assignment and reporting. Policy period deductibles, premium, payroll, and other information are tracked for each contract period. Other features include:
  - Excess and reinsurance tracking
  - Coverage assignments to multiple locations
  - SIR by claim, by occurrence, and various reporting levels

- Organizational Hierarchy - iVOS supports up to 20 levels of organizational hierarchy, including the ability to define relationships between entities within an organization. Assignment of a claim to an organizational level is accomplished using a directory tree (similar to Windows Explorer) that displays each level as a folder with expandable sublevels. Selecting a sublevel enables that claim's financial and other information to roll up in reports under the parent organizational levels.

- Litigation Tracking - iVOS has a litigation tracking window that enables multiple lawsuits to be tracked, with multiple claimants and attorneys associated with the suit. This screen comprises extensive information, including demand amounts, hearing dates, court assignments, and more. Business rules can be configured based on dates entered in the litigation management window to notify system users (via diaries) or external partners such as defense attorneys (via e-mail) of upcoming hearings or trials. iVOS also has a Litigation Calendar that displays daily, weekly, or monthly litigation activity across multiple suits, claims, and counsel, using an interface similar to Microsoft Outlook. The calendar also has a filter that allows the user to show only activities of a particular type or involving specific counsel, dates, and so forth.

- Case Load Management - This functionality will help a supervisor review each examiner's cases, and easily re-assign claims to another examiner by highlighted the claims to be moved, selecting the Assign Examiner button, and deciding which examiner, supervisor, or adjusting office to move claims to, and whether or not to move diaries assigned to the claim file.

- Reporter Module (includes Report Design Tool & Report Distribution) – iVOS provides a broad range of standard report templates designed to enable users to analyze data from and insurance and risk management perspective. Reports can be run using diverse

filtering and grouping options, and the report output can be saved for future reference or for distribution. Data can also be downloaded to excel for further analysis. The Report Design Tool can be used to modify existing standard report templates or to create a new report from scratch without any programming assistance. Report Distribution allows for the batch scheduling of electronic reports to be generated without user intervention.

- Scheduler – This module is used to configure, schedule, run and manage all jobs, processes, routines, services, etc., that need to be run on a regular or occasional basis. Examples are payment processing and check printing, report generator, import and export jobs. iVOS Scheduler features includes job chaining, error handling, e-mail error notification, and schedule monitoring.

- Claim Mail – iVOS Mail is a fully integrated e-mail system within iVOS that associates an e-mail account with each claim file. Sending an e-mail from a claim uses an interface similar to Microsoft Outlook, with comparable address book, text entry, and file attachment capabilities. Replies to iVOS Mail messages are automatically placed in the claim file's iVOS Mail inbox (only displaying e-mail associated with only the one claim), as well as the user's iVOS Mail inbox (which displays e-mail from all claims). While viewing a claim-related e-mail in his or her user inbox, the user can navigate directly to the claim file by double-clicking a link in the message. [disclaimer - email in and out of iVOS is based on client's email system and their security……Ventiv has no liability around email system]

- Guest Links - E-mail generated by iVOS (via either Claim Mail or business rules) can include a "guest link" that provides the recipient with single-click access to the referenced iVOS claim file, even if the recipient is not an iVOS user—all he or she needs is a web browser and an Internet connection. This feature enables examiners to share claim information online in real time with lawyers, investigators, nurse case managers, etc., without having to mail hard copies of the claim file. [disclaimer - email in and out of iVOS is based on client's email system and their security……Ventiv has no liability around email system]

- Medical Case Management – to track the referral of claims for nurse case management, including triage of the case, medical authorization, utilization review savings, and time tracking.

- Security and Configuration Administration - iVOS uses role-based security to completely configure the user interface for the various workgroups that will be accessing the system. Each role can be defined by hiding tabs and fields, setting fields as read only, re-labeling field names, hiding columns of data, restricting access to data in tables, hiding items in drop down menus, etc.

- Complete Audit Trails - In order to preserve a comprehensive audit trail of transactions and information in iVOS, any modification to claim data is logged with the user ID and timestamp. Both the creation of and changes to payments, reserves, diaries, notes, correspondence, and e-mail are all tracked by date/time/user stamp information. To ensure an accurate audit trail, there is no delete button on any claim-related page in the system. In addition, iVOS Full Table Auditing functions provides clients with the ability to log all field changes and have an ongoing audit function. A user can search the Audit Logs and view log items. A search tool is provided on the Full Table Audit tab to enable users to quickly and easily access the edit logs they need to view.

B. Optional Modules

- ISO ClaimSearch Interface – Two-way interface with ISO that identifies claim histories of insureds and claimants to assist in the adjustment of claims and detection and prevention of insurance claim fraud. When Customer submits a claim, it will automatically receive any applicable matches along with other system information that helps verify data submitted as part of the claim report. Customer will be responsible for obtaining a license from ISO for the ISO functionality accessed by the ISO ClaimSearch Interface.

- CA Commutation Calculator – Incorporates the California Commutation Calculator for present value calculation of Permanent Disability per Labor Code §§5100-5106. Multiple calculations can be stored on each claim. Calculation results can then be copied to the scheduled payments for the remainder (if any) of the award. The commuted amount can also be copied to the payment window for payment processing.

- Check Printing Module – Provides high-quality printing of custom-designed checks using an existing laser printer and stock paper, including the capability to combine multiple payments per check according to Customer's specifications. The module also includes custom graphics and gives Customer control over different check stocks for different accounts.

- Electronic Funds Transfer – The ability to make payments directly into a claimant's bank account.

- Document Imaging Module – Enables the attachment of scanned documents to iVOS claim records. The iVOS imaging workflow is highly configurable and can be tailored specifically to handle Customer's interface/integration requirements. iVOS can be configured to save images either in the claims database, or in a file structure.

- ODG Reserve Analysis – Provides the capability to electronically import data from the Work Loss Data Institute (WLDI) on a regularly scheduled basis. In addition, clients can configure iVOS to generate reserves automatically based on certain criteria. Customer will be responsible for obtaining a license the data directly from WLDI.)

- Customer Invoicing - Provides the ability to invoice customers for claims administration services, by taking time entries that have been created by users on individual claims files (time tracking) module),and applying customer contract information (contract tab for Customer) to product an invoice.

C. Optional Interfaces

- Employee Interface – iVOS has a standard employee import interface (fixed-width flat file). When a claim (or injury report) is opened and a Social Security or employee number is entered, the employee information is automatically populated into the general claim window, eliminating the need to manually enter the data.

- Positive Pay/Reconciliation Interface – Two-way electronic transfer of check information between iVOS and Customer's bank. Information exported from iVOS (Positive Pay) informs Customer's bank as to which checks have been issued, for how much, and to whom. Files imported from Customer's bank (Reconciliation) identify cleared checks and corrections, which are then applied to individual payments in iVOS. (fixed-width flat files). A fixed-width flat file

- Claim Intake Interface – A fixed-width flat file that imports basic claim information or first report of injury/incident information from an external third-party system, such as a call center solution. This information is mapped into the appropriate fields, triggering business rules to initiate the claim workflow process. This is claim information only and only one claimant for one claim.

- Vendor Interface – A fixed-width flat file that imports basic vendor information from an external third-party system, such as an accounts payable system.

- Document Image Import – A fixed-width flat file that imports images from an external third-party system. The interface is in an ACORD-based format.

- Company Nurse Interface - A fixed-width flat file that imports basic claim information or first report of injury/incident information from Company Nurse. This information is mapped into the appropriate fields, triggering business rules to initiate the claim workflow process. This is claim information only and only one claimant for one claim.

- Policy Interface - A fixed-width flat file that imports policy information from an external third-party system, such as a policy administration system.

- Organization Interface - A fixed-width flat file that imports organization information from an external third-party system.

- Notes Interface - A fixed-width flat file that imports notes from an external third-party system.

- 3rd Party Interface Bill Review (Import & Export) - A fixed-width flat file that imports and exports bill review information. Claim and Vendor information is exported from iVOS and Payment and Fee information is imported into iVOS.

- ISO Fee Import Interface – allows the ISO Fees to be imported into iVOS so they can be applied to the claim file.

D. Compliance Modules

- CMS Reporting Module – Includes several iVOS scheduled jobs and business rules for processing the mandatory claims data to meet Section 111 reporting requirements. Features include assigning/managing Responsible Reporting Entity (RRE) IDs, running data validation reports, generating export files, importing CMS responses, and updating claims, as well as notifying adjusters of data validation issues and claim updates

- EDI FROI – iVOS includes a standard interface to support state-mandated workers' compensation EDI and fully supports IAIABC Release 1, 2 and 3 transmission requirements. The interface will produce an export file that contains data formatted for transmission to the appropriate jurisdiction. Specific supported states are indicated in the Order Form in Schedule B.

- EDI SROI – Supports requirements for mandated EDI reporting of the SROI. The interface will produce an export file that contains data formatted for transmission to the appropriate jurisdiction. Specific supported states are indicated in the Order Form in Schedule B.

E. iVOS User Types & Access Rights

A. "Concurrent Full Access Users" means the total number of users of the Software who have full access rights to the Software who are allowed to access the Software on a concurrent basis. Customer may have any number of users with full access to the Software, but only up to the total number of full access user licenses may be using the Software at any one time, regardless of being remote or local.

B. "Concurrent Read Only Users" means the total number of users of the Software who can only read information in the Software Product and use iVOS Reporter, but cannot update or add any information. Unless a Customer changes iVOS security to restrict iVOS Reporter from a "read only" user, such users will have access to iVOS Reporter.

C. **"Concurrent Report Only Users"** means the total number of users of the Software who only have use of the Reporter function of the Software Product. The Customer would be required to use administrative tools to restrict access to all other functions of the Software other than iVOS Reporter module as well as ticking the box to describe them as a "read only" user to ensure that such "Report Only" user is not counted against a concurrent license.

D. **"Concurrent Guestlink Users"** means the total number of users of the Software who the Customer has granted Guestlink access through ClaimMail who can read, update or add information in the Software Product. Their level of access depends on the level of security defined by the Customer. **If the guest link user is set up as a Read Only User, then that user will not count as a "Concurrent Full Access User," otherwise that user will count against the total number of Concurrent Full Access Users**.

II. Capture.

The incident intake forms tool for incidents known as Ventiv Capture will allow Customer to capture data with this reporting tool as further described in the Statement of Work **("Capture")**.

III. RiskConsole Advance®

.

A. RiskConsole Advance® Modules Available for Order by Customer

Summary Exposure Values

Operational Summary exposure data can be captured, tracked and summarized at any level within the organizational hierarchy (division, region, district, community, etc.). This data can be updated via systematic data loads, manually entered by end-users, or by utilizing our unique spreadsheet update functionality. This information can be used to assist in the renewal process as well as be used as an internal benchmark for reports (revenues, hours worked, sales, employee concentration, etc.).

Occurrence Module

RiskConsole Advance's Occurrence Module relates all claims associated with an event or accident. RiskConsole has a flag on the claim record that denotes if a claim is the lead claim for the occurrence. There may only be one lead claim on the occurrence. This allows for reporting at an occurrence or claim level.

Claims Management Module

RiskConsole Advance's Claims Module is a comprehensive claims management system for managing the life cycle of a claim from pre-loss incident through claim closure and settlement with full status and financial audit of the process. Claim/incident records as well as corresponding fields can be viewed, edited, created, or deleted as dictated by security privileges assigned to the user. Field level security can be further restricted to protect sensitive information from being displayed or edited as necessary. Users can record all status value changes, financial reserving and settlement information with transaction support for payments. Provisions are provided for tracking/recording all loss descriptor information such as cause, nature and body part for Safety/Loss Control purposes. Occurrence support is provided for linking multiple claims associated with an event or accident. RiskConsole has a flag on the claim record that denotes if a claim is the lead claim for the occurrence. There may only be one lead claim on the occurrence. This allows for reporting at an occurrence or claim level. The Claims Module also includes support for claim notes, diary tasks and file attachments. Claim information can be linked to other information being tracked in RiskConsole, i.e. contacts, properties, fleet, etc.

OSHA and Occupational Employee Absence

The Occupational Employee Absence Module is associated to the claim record and allows for tracking of employee absence details. This information will be used to drive OSHA reports. OSHA specific fields are tracked on the claim record.

MMSEA Module

Section 111 of the Medicare, Medicaid, and SCHIP Extension Act of 2007 (MMSEA) (P.L. 110-173), adds mandatory reporting requirements for liability insurance (including self-insurance), no-fault insurance, and workers' compensation. Ventiv's solution is to provide clients ability to capture, export data for self-reporting, then process CMS response as provided.

Employee Module

The Employee Module allows for tracking of employee details including name, address, birth date, wage information, etc. In cases of single sign-on to RiskConsole, the employee file is also used to create and maintain user login security within RiskConsole.

Litigation Module

The Litigation Module (Matter Management module) guides an organization's internal legal staff in managing financial data, matters and documents in one secured system. The module tracks legal actions brought against a company including docket details, allegations, attorney, diary information and litigation-specific financials allowing you to strategically manage your legal matters with greater insight into performance, expenses and risk. Litigation information can be linked with incident, claim, safety, policy and exposure information to provide a single comprehensive environment for data management, risk analysis and risk reporting.

Property Management Module *(NOTE: If you have Property Recommendation or Full Property, then delete this section)*

The Property Module is a comprehensive property management system that captures all COPE (construction, occupancy, protection, exposure) information and detailed financial information. RiskConsole Advance's property module pushes the data collection responsibility to field users who are most knowledgeable of their exposures and enables them to update their location information at any time.

Full Property Module *(NOTE: If you have Property Management, then delete this section)*

The Full Property Module is a comprehensive property management system that captures all COPE (construction, occupancy, protection, exposure) information, detailed financial information, surveys and recommendation information. RiskConsole Advance's property module pushes the data collection responsibility to field users who are most knowledgeable of their exposures and enables them to update their location information at any

Environmental Module *(NOTE: Must have one of the Property modules to have this)*

RiskConsole Advance's environmental module tracks and warehouses environmental, legal, and insurance documents associated with individual properties and portfolios. Key attributes include: real-time access to environmental coverage, enhancements, deductibles, limits, and property claim history.

Renewal Module *(NOTE: Must have one of the Property modules to have this)*

The renewal module allows customers to collect information commonly requested by underwriters from users in the or related to the annual renewal of that insurance program. The module includes an extensive set of questions that have been commonly identified to be required to renew a casualty or property program. ***The module will only include these standard questions unless the customer has designated a different set of questions in Appendix A to the Statement of Work.***

Policy Management Module

RiskConsole Advance's Policy Management Module provides the ability to track policies and understand the premium spending, coverage afforded (deductibles and limits) and identify the insurers providing the coverage. Customer also has the ability to manage all the aspects of the policy structure including:

- Policy header- basic policy details including period of policy, policy description, premium and any policy level limits or aggregates.
- Policy sections- identify coverages involved with respective deductible, limits and portion of Organization covered.
- Policy participants- insurers and optionally re-insurers involved and their respective share of the coverage.
- Policy variations- identify variances in coverage within a section.
- Combined Limits- identify any combined limits between policies.

The following standard capabilities are available for use as needed:

- Program/Layer Support: the Customer can define their programs and layers so that the physical policies in place can be viewed in relation to the Customers program structure.
- Premium Payments: track the premium payments for the policy.
- Claim Link: Use the Policy details to identify insurance coverage on a claim, with a specific link from the Claim to Policy and establishing the deductible and limits applicable to the Claim per the Policy definition.
- Policy Performance: Manage the performance of the Policy in terms of the aggregate claim financials, loss ratio and managing of basic aggregates. Note this capability is limited to the Claims connected to the Policy and does not cater for linked Policies in the program (see Risk Financing module for expanded capabilities).

Premium Calculation / Allocation

RiskConsole Advance's Allocation Module will allow Customer to calculate and/or allocate premium across coverages and organizations within RiskConsole. With respect to Allocation, the global amount of premium is always known and recorded at the policy level. RiskConsole will be used to split this global amount across the coverage and the organization. In the Calculation model, RiskConsole will calculate all detailed premiums and, once summarized, will provide the global amount of premium by policy. A data process will be scheduled to run on a specified time interval to calculate and/or allocate the premium.

Insurer Ratings Module

The Insurer Ratings Module consolidates rating data from multiple sources (S&P, AM Best, and Ventiv MARS) and provides those ratings per the client's active insurers. Customer has view access only to the Insurer Ratings information.

Contract Module

RiskConsole Advance's Contract Module allows for tracking contractual relationships including contract number, vendor names, addresses, contract detail, contract period, contract value, contract type, etc. This module can automatically reminds Customer of contract expirations, new contracts entered and reminders associated with contracts. This module can also house contract attachments including version control.

Fleet Module

The RiskConsole Fleet and Driver Module provides a tool to consolidate all fleet details (VIN #, Make, Model, Type, etc...) into one central repository for management. Many clients use the Fleet Module to manage complete maintenance and repair schedules for their entire fleet. A specific VIN can be tied to one or multiple drivers, and then be associated to a claim, providing the ability to search for a VIN, and see all associated drivers and claims to that particular vehicle, with the click of one button.

Risk Register Basic

Ventiv Technology has developed the Risk Register module in RiskConsole, offering a sophisticated alternative to a spreadsheet approach, while being less expensive and resource-intensive than a dedicated enterprise risk management solution. It is simple and clear, scalable, easily accessible and flexible, providing "heat map" analysis of the risks you face. It allows clients to track the risks associated with the organization's business and rank the likelihood and financial impact of these risks.

Risk Register Enhanced

The enhanced module includes the functionality available in the Risk Register Basic module and also includes the ability to track risk controls and associated actions used in managing these risks.

Clinical Trial Management Module

The workflow around the certificate forms and notifications will be defined with Customer. The certificates will utilize the word/mail merge functionality of RiskConsole.

B. RiskConsole Advance® User Types & Access Rights

		Type of User			
		Lite/Incident Entry (L)	View User (V)	Full User (F)	Administrator (A)
Functionality	**Add Records**	X	N/A	X	X
	Edit Records	X	N/A	X	X
	View Records	X	X	X	X
	E-Mail Individual Records	X	X	X	X
	Add Attachments to Records	X	N/A	X	X
	Quick Search	X	X	X	X
	Use Mail Merge Templates	X	N/A	X	X
	Create Mail Merge Templates	N/A	N/A	Option	X
	View Report/Dashboards	X	X	X	X
	Download Reports to Excel	X	X	X	X
	Drill through from Report to Record Detail	X	X	X	X
	Advanced Query	N/A	N/A	X	X
	Run/schedule existing report templates	N/A	N/A	Priced Option	X
	Query Studio	N/A	N/A	Priced Option	Priced Option
	ReportStudio	N/A	N/A	Priced Option	Priced Option
	Mapping	N/A	Priced Option	Priced Option	N/A
	Spreadsheet Update	N/A	N/A	Priced Option	X
	Spreadsheet Import	N/A	N/A	Priced Option	Priced Option
	Workflow Automation	N/A	N/A	Priced Option	X
	Delete Records	N/A	N/A	Option	Option
	Manage Hierarchy/Lookup Values	N/A	N/A	N/A	X
	Administration Options: User Management, Group Management, Exchange Rates	N/A	N/A	N/A	X

Schedule B to the Software License & Support Agreement

Initial Order Form (iVOS – hosted, RiskConsole Advance, Capture)

I. Initial Maintenance Term. The Initial Maintenance Term of the Agreement will commence on the Effective Date and continue through the end of the sixtieth (60^{th}) month thereafter.

II. Initial Hosting Term. The Initial Hosting Term of the Agreement will commence on the Effective Date and continue through the end of the sixtieth (60^{th}) month thereafter. The Initial Hosting Term is also the term of the Access License granted in Section 3.2 of the Terms and Conditions.

III. Software Modules. Ventiv licenses the selected Software modules indicated below to Customer in accordance with the terms and conditions of the Agreement.

iVOS			
iVOS Claims Administration Modules		**Optional Interfaces**	
■	Workers' Compensation Module	■	Employee Interface
■	Property and Casualty Module	☐	Positive Pay/Reconciliation Interface
☐	Disability Module	☐	Claim Intake Interface
☐	Event Management Module	☐	Vendor Interface
Optional Modules		☐	Document Image Import
☐	ISO ClaimSearch Interface	☐	Company Nurse Interface
☐	CA Commutation Calculator	☐	Policy Interface
☐	Incident Reporting	☐	Organization Interface
☐	Check Printing Module	☐	Notes Interface
☐	Electronic Funds Transfer	■	3rd Party Interface Bill Review (Import & Export)
■	Document Imaging Module	☐	iVOS/SmartAdvisor SSO (Single Sign On
☐	Central Output Management Module	☐	ISO Fee Import Interface
☐	ODG Reserve Analysis	■	Accounts Payable Interface
☐	Multi-Currency	**Compliance Modules**	
☐	Claim Invoicing	■	CMS Reporting Module
☐	Customer Invoicing	■	EDI FROI for Colorado
☐		■	EDI SROI for Colorado
		☐	NCCI Medical Data Call
RCA & Capture			
Advanced Safety & Analytics (RiskConsole Advance)		**Intake Forms**	
■	Claims	■	Capture
■	Action Items		
■	Investigations		
■	Root Cause Analysis		
■	Safety Meeting/Training Tracking		

IV. Number of Users/User Types. Customer's license to the Software is limited to the following number of users and user types:

Type of User*	# of Users	Cost for Additional Users
Concurrent Full Access iVOS Users	**20**	**Then current rates**
Concurrent Read Only iVOS Users	unlimited	n/a
Concurrent Report Only iVOS Users	unlimited	n/a
Concurrent Guestlink iVOS Users	unlimited	n/a
Incident/Event Intake Capture Users	unlimited	n/a
Administrator Capture User	1	**Then current rates**
Administrator RiskConsole Advance	1	**Then current rates**
Lite Safety Users RiskConsole Advance	20	**Then current rates**

***** *User types are described in Part II of Schedule A*

V. **Data**

A. RiskConsole Advance One Time and Ongoing Data Loads. – Ventiv will provide the following ongoing production data loads on the frequency described below:

Module	Date Received From	File Type	Frequency	Data Load Type
Organization	iVOS	Standard	Daily	Snapshot
Claims / Incidents	iVOS	Standard	Daily	Transactional
Safety Meetings	Excel	CSV/Excel	One Time	Snapshot

B. iVOS Data Conversion. Ventiv will provide the following historical conversion of data.

Module	Date Received From	File Type	Frequency	Data Load Type
Insured Policy Data	CS Stars	Database (Oracle) or ASCII Format	Worker's Compensation Liability	New Implementation
Core Claim Data	CS Stars	Database (Oracle) or ASCII Format	Worker's Compensation Liability	New Implementation
Financial Data	CS Stars	Database (Oracle) or ASCII Format	Worker's Compensation Liability	New Implementation
Contacts, Diaries, Notepad, Litigation, Vehicle, EDI, Work Status, and associated reference tables	CS Stars	Database (Oracle) or ASCII Format	Worker's Compensation Liability	New Implementation
Document Images	CS Stars	Database (Oracle) or ASCII Format	Worker's Compensation Liability	New Implementation
Document Images – Medical Records	SharePoint	Database (Oracle) or ASCII Format	Worker's Compensation Liability	New Implementation

i. Conversion of up to 78,000 Claims.
ii. Conversion of up to 35,000 Images.
iii. Cost estimates are based on an anticipated total record count of up to 250 gigabytes of storage during the proposed contract period (including all RiskConsole Advance and iVOS)

Data Storage. Effective April 20, 2018, Data Storage Fee includes 250 GB of data storage. Additional storage will be charged at the rate of $750/GB/year on each anniversary of the Effective Date of the Master Service Agreement. At the end of each quarter, Ventiv will report to Customer the amount of storage being utilized by Customer."

VI. Capture

A. Deliverables:
i. 5 Custom Intake Forms (1 Language)
ii. Capture Intake, Capture Native App – Apple iOS or Capture Native App – Google Android

VII. Setup/Deployment Services. The Statement of Work set forth in Attachment 1 to this Agreement describes the Setup/Deployment Services to be provided by Ventiv to Customer under this Agreement.

VIII. Managed Service Hours. Customer will receive 200 hours Managed Service Hours on an annual basis.

IX. Fees. Ventiv will invoice and Customer will pay the following Fees:

A. Non-recurring Fees - Estimated one-time fees comprised of the following:

i. ***Setup / Deployment: 705 hours ($52,224)***

a. Data Conversion

The pricing estimate is based upon an estimated number of hours. Additional conversion costs will be invoiced monthly on a time and expense basis as incurred.

b. Training:

Additional training costs will be invoiced monthly on a time and expense basis as incurred.

ii. ***Consulting: 1026 hours ($75,776)***

Hours estimated in the SOW for the following setup/deployment services:
- Project Management
- Business Analyst General Services; Base installation, Conversion tasks, base setup, interfaces, Report Analysis
- Business Analyst Hours Configuration services
- Report Development services
- Intake form setup and configuration

Resources for project management and Setup/Deployment support vary based on the project requirements

The pricing estimate is based upon an estimated number of hours. Additional implementation costs will be invoiced on a monthly basis as incurred.

B. Annual Recurring Fees - Comprised of the following:

i. **Subscription Fee: $198,500 (first year)**
ii. **Data Services**
iii. **Customer Support**
iv. **iVOS Hosting** (based on contracted number of users and 250 gigabytes of Data Storage). Additional Users and Data Storage will incur additional Annual Recurring Fees.
v. **Managed Service Hours** (based on 200 hours per year), excluding travel and expenses.
vi. **Other Annual Fees:**
    1. **Annual Stewardship at client site for 1 person**

Total Annual Recurring Fees: ($198,500)

C. Additional Fees.

- Additional Setup/Deployment Services are available at Ventiv's then-current hourly or block hour rates.
- Additional hours for Customer Support Services are available at Ventiv's then-current hourly or block hour rates.
- Additional Training Services available at Ventiv's then-current hourly or block hour rates.
- Travel and expense costs associated with all services will be billed as incurred.
- Annual stewardship meeting at Customer's site available billed via Managed Service Hours plus travel and expenses.

X. Payment Schedule.

A. Setup/Deployment & Consulting Fees. Ventiv will invoice Customer for the non-recurring Setup/Deployment & Consulting Fees on the following milestone dates:

i. **Setup/Deployment Fees.** Ventiv will invoice Customer for the non-recurring Setup/Deployment Fees on the Effective Date.
ii. **Consulting Fees.** Ventiv will invoice Customer for the non-recurring Consulting Fees based on the following milestone dates:
    1. 1 January 2019
    2. 1 March 2019
    3. 1 May 2019
    4. 1 August 2019

B. SaaS License, Support, Hosting, and Managed Service Fees. Ventiv will invoice Customer for the License Fees upon the Effective Date.

C. Travel & Expenses. Ventiv will invoice Customer for all travel and expense costs on a monthly basis as incurred.

XI. Total Fees per Year to be Paid as of Effective Date

The table below indicates what that the total fees will be in Years 1-5.

Year	Total Fees Payable	Non-Recurring	Annual Recurring
Year 1	$ 326,500	$128,000	$198,500
Year 2	$204,455		$204,455
Year 3	$210,589		$210,589
Year 4	$216,906		$216,906
Year 5	$223,414		$223,414

Schedule C to the Software License & Support Agreement

Support & Hosting Service Levels Schedule (iVOS Hosted Model)

1. **Definitions.**

1.1 "**Business Hours**" means the hours of 8:00am to 9:00pm Eastern Time on all Business Days.

1.2 "**Customer's Support Contacts**" has the meaning set forth in Section 6 of this Schedule C.

1.3 "**Error**" means a material failure of the applicable Software to conform to the functional specifications described in its Documentation.

1.4 "**Error Corrections**" means any modification, workaround, or routine intended to correct the practical adverse effect of an Error.

1.5 "**Excusable Downtime**" means the total minutes in the Measurement Window during which the Software or the Hosting Environment (as applicable) was not available due to (a) any negligent or wrongful act or omission by Customer or its users; (b) any negligent or wrongful act or omission by Third-Party Vendors; or (c) any force majeure events or disruption in public internet access.

1.6 "**Follow-up Frequency**" means the frequency of time that a support consultant will update the customer (electronically or otherwise) on the progress of commercially reasonable efforts to resolve an issue.

1.7 "**Hosting Environment**" means the data center and related infrastructure encompassing the Software and System as a whole maintained by Ventiv, including the data loading servers and application reporting servers as well as the system servers.

1.8 "**Measurement Window**" means a period of thirty (30) days.

1.9 "**Recovery Declaration**" means the time period in which a disaster would be declared and recovery plans are enacted.

1.10 "**Release**" means a modification of the Software, normally denoted with a new number to the immediate right or left of the decimal, which contains new features and functionality. Release does not include new products or modules of the Software for which Ventiv generally charges its customers an additional license or subscription fee.

1.11 "**Response Time**" means the amount of time from when the customer properly reports an issue until a support consultant acknowledges receipt (electronically or otherwise) and initiates troubleshooting to resolve.

1.12 "**Resolution Goal**" means the amount of time that is set as a goal to resolve an incident. Commercially reasonable efforts will be used to meet this goal.

1.13 "**RPO**" means Recovery Point Objective, which is the maximum amount of time for potential data loss in the event of a disaster.

1.14 "**RTO**" means Recovery Time Objective, which is the period of time to restore services from point of Recovery Declaration.

1.15 "**Scheduled Downtime**" means the total number of minutes of actual time the Software or Hosting Environment, as applicable, were not available as a result of scheduled time to perform system maintenance or Patches.

1.16 "**Severity Level**" means the impact level assigned to an issue based on the level of service degradation or loss of functionality.

1.17 "**Patches**" means a change to the Software that may include patches, fixes, minor updates and Error Corrections, which Ventiv generally provides to its customers who receive customer support services.

1.18 "**Unscheduled Downtime**" means total number of minutes of actual time the Software or Hosting Environment, as applicable, were not available, which does not qualify as Scheduled Downtime, but specifically excludes any Excusable Downtime.

2. **Support Generally.**

2.1 Ventiv will provide one or more reasonable means of communication to allow Customer's Support Contacts to contact Ventiv for assistance in resolving problems with the Software ("**Help Desk**") in accordance with and during the hours of operation more specifically set forth in this Schedule C. The Help Desk will allow communication in accordance with the table set forth in Section 7 below.

2.2 Because Customer has no rights in the source code version of the Software, and may only use the object code version of the Software, Customer may only maintain the Software at the administrative level and then only in a manner that will not cause corruption of the code. Customer is prohibited from attempting to support the Software (either itself or through a third party) in any way that would require access to the source code of the Software or would require any reverse engineering, reverse assembly or disassembly of the Software. Ventiv currently is the only entity authorized to support the Software at the code level and does not provide any of its customers the right to access the source code in order to support the Software.

2.3 Ventiv will provide Customer Support Services for the "current release" and "previous release" (major or minor). The "end-of-life" ("EOL") release will be eligible for emergency, external-driven interface changes with less than three (3) months' notice and defect resolution for issues of severity 1 – 3 to allow Customer to upgrade from the "EOL release" to either the "current release" or the "previous release."

3. Support and Maintenance.

3.1 Services. Subject to the timely payment of the applicable Subscription Fees set forth in the Order Form, Ventiv will provide the level of support identified herein in accordance with the support descriptions set forth below. Ventiv will notify (electronically or otherwise) Customer of any changes to such support descriptions in each subsequent renewal, as applicable. No other maintenance or support for the Software is included in this Agreement.

3.2 Fees. Subscription Fees will be due and payable in accordance with this Agreement. Subscription Fees are non-refundable, once paid to Ventiv.

4. Error Corrections and Patches.

4.1 As a part of the Customer Support Services, Ventiv will use commercially reasonable efforts to provide Error Corrections for all verifiable and reproducible Errors in the Software in accordance with the Agreement and this Schedule C.

4.2 As a part of the Customer Support Services, Ventiv will provide Patches to the Software that Ventiv makes generally available to its customers who receive support services.

5. New Releases.

5.1 As a part of the Customer Support Services, Ventiv will provide to Customer new Releases of the Software as and when developed, except for new products or modules for which Ventiv generally charges a separate license or subscription fee. Ventiv is not obligated to develop new Releases of the Software.

5.2 Ventiv will provide Customer, as part of the Customer Support Services, with new Releases created by Ventiv as a result of a change in law or new law that directly applies to existing functionality within the Software currently offered by Ventiv. As an accommodation and not as provision of legal advice, Ventiv will take commercially reasonable efforts to promptly notify Customer in writing upon becoming aware of any material changes to any applicable law or governmental regulations that may cause the current Release of the Software not to conform to such law or regulations. Notwithstanding the foregoing, in the event that the required modifications to the Software (i) would require a material re-architecture or other significant product re-design, (ii) would require Ventiv to obtain data which is either unavailable, or, which is only available at a material cost, or (iii) would otherwise require Ventiv to incur material expenditures (as measured against the fees charged under this Agreement), and Ventiv is not otherwise making such modifications for its other customers, then Ventiv may cease providing the affected Software in the affected jurisdiction. Customer is strongly encouraged to consult with its own attorneys and other advisors as to legal requirements in effect from time to time.

5.3 In the event that Ventiv intends to withdraw any Software from general availability for any reason whatsoever, Ventiv will provide Customer at least six (6) months prior written notice of such withdrawal.

6. Software Upgrades.

6.1 Ventiv provides utilities, scripts and documentation to enable self-hosted Customers to upgrade their own test and production environments. Ventiv hosted Customers are entitled to one (1) test and one (1) production non-compliance related upgrade per year, included in their Subscription Fee.

6.2 Ventiv-hosted Customer upgrades include: (a) scheduling the upgrade with the Customer contact; (b) applying upgrade scripts to the test environment during Ventiv's business hours; (c) completing a backup of the production data before the upgrade; and (d) upgrading the Customer's production environment during normal Ventiv business hours. The Customer is also entitled to one (c) test database refresh from production data per year by Customer request.

6.3 If the upgrade request is outside of the scope of this Agreement as indicated in Sections 6.1 through 6.2 above, Ventiv will notify the Customer to that effect and reserves the right to charge Customer at Ventiv's then current standard hourly rates, for which Customer agrees to pay Ventiv promptly upon receiving an invoice. The following are examples of upgrade requests that are available from Ventiv: (a) Customer requested test refresh database from production data in addition to the one refresh per year (Ventiv-hosted Customers only); (b) additional upgrades in test or production environments required by the Customer through no fault of Ventiv; (c) upgrade or upgrade activities requested during non-business hours; (d) request for Ventiv to perform the test and/or production upgrades for self-hosted Customers.

7. Limitations.

7.1 Ventiv is under no obligation to provide Customer Support Services with respect to: (a) Software that has been altered or modified by Customer or any third party; (b) Software used on a system that does not meet the minimum hardware, software, operating system, mobile device, and other system and configuration requirements set forth in the Documentation or provided by Ventiv; and (c) any software not both supplied by Ventiv and identified on an Order Form.

7.2 Customer Support Services does not include researching Customer requests, researching and fixing anomalies caused by other vendors, making changes resulting from internal Customer business practices, enhancing system configuration and other similar tasks that are requested or required, but are outside of Ventiv's control. Causes or errors that are not attributable to Ventiv (and therefore would also be considered Additional Services) include, but are not limited to, the following: (i) accident; unusual physical, electrical or electromagnetic stress; neglect; misuse; failure or fluctuation of electric power, air conditioning or humidity control; excessive heating; fire and smoke

damage; or causes other than ordinary use; (ii) use of the Software on equipment or rotation media other than the equipment for which such software was designed and licensed for use on; (iii) interconnection, interfacing or operation of the Software with other software products not supplied by Ventiv; (iv) operation of the Software with other media, hardware, software or telecommunication interfaces not meeting or not maintained in accordance with the manufacturer's or environmental or Ventiv's specifications; (v) improper installation by the Customer or use of the Software that deviates from any operating procedures established by Ventiv in the applicable Documentation or in environmental or manufacturer specifications, for example, virtual machine configuration; (vi) modification, customization, alteration or addition or attempted modification, customization, alteration or addition of the Software undertaken by the customer or its agents, assigns, contractors, employees or other's under the customer's control (vii) software programs made by Customer or other parties unless specifically covered in a Statement of Work between the Customer and Ventiv; (viii) Customer's failure to implement current versions of the Software that are issued under this Agreement; (ix) introduction of data into any database used by the Software by any means other than the use of the Software; (x) failure by Customer to respond to any action plans provided by Ventiv pursuant to a support call by Customer; (xi) improper or incomplete J2EE application server administration; or (xii) improper or incomplete database administration.

7.3 If Ventiv has created a third party interface ("**Third Party Interface**") to one of Customer's third party products provided by another vendor ("**Third Party Product**") and such vendor modifies the Third Party Product causing the Third Party Interface to stop functioning properly, then the services required to modify the Third Party Interface as a result of the changes to the Third Party Product are considered outside the scope of Customer Support Services and would incur additional fees in accordance with Section 5.4 below. Services required to resolve any Customer-Created Error are outside the scope of Customer Support Services and would incur additional fees in accordance with Section 5.4 below.

7.4 If a problem reported is outside the scope of this Agreement as indicated in Sections 5.1 through 5.3 above, Ventiv will notify Customer to that effect and reserves the right to charge Customer at Ventiv's then current standard hourly rates, for which Customer agrees to pay Ventiv promptly upon receiving an invoice. Certain requests, such as building custom modules, database objects, reports, utilities or other complex projects ("**Additional Services**") may also incur additional fees beyond those associated with Customer Support Services and will be detailed in a new Order Form and Statement of Work agreed between the parties and subject to the terms and conditions of this Agreement. The following are examples of Additional Support Services that are available from Ventiv: (i) add-on data conversions; (ii) implementation for any optional software modules; (iii) supplemental training; (iv) custom reports – defining, creating, testing or troubleshooting (Ventiv will help with "how do I add a table, column, field, etc." in Report Designer, but Ventiv will require a Statement of Work to help troubleshoot or clean up a modified or custom report (unless the custom report is specifically under maintenance; for example: "I tried to add to or modify my custom report and now my outstanding indemnity figures are incorrect")); (v) iVOS upgrades during non-business hours; (vi) security configuration consulting or setup; (vii) data conversion issues once transitioned from implementation to support; (viii) Ventiv database changes, such as organization changes, combining insureds, reference table changes, *etc.*; (ix) corrections to Customer's data, including, but not limited to, data modification for purposes of exporting/importing to/from the Ventiv database; (x) database administration services (iVOS self-hosted only); (xi) J2EE application administration (iVOS self-hosted only); (xii) backup and recovery consulting (iVOS self-hosted only); (xiii) performance troubleshooting outside of the application; (xiv) any hardware or software problems beyond the control of Ventiv; (xv) network changes and network performance problems (xvi) support and maintenance of custom modules that are not covered under the Customer Support Services; (xvii) custom enhancements, for example: new check printing functionality or custom-stored procedures (*e.g.*, examiner); and (xix) for iVOS interfaces: (a) installation and configuration of any interface Software on hardware external to the Software server; (b) training on interfaces; (c) Customer-initiated changes to the interface specification (note that Ventiv reserves the right to modify the interface specification for future enhancements); (d) Customer changes to systems external to Ventiv that result in any failures or performance problems with the interface; or (e) bugs in a Customer's computer software and hardware that result in interface operational failure.

7.5 The following types of requests will incur additional fees: (I) password resets; (ii) performance troubleshooting outside of the application; (iii) any hardware or software problems beyond the control of Ventiv; (iv) Customer network changes and network performance problems; (v) training questions; and (vi) documentation requests for documents available on the portal or online help.

7.6 Support is delivered in English only, unless Customer is in a location where Ventiv has made localized support available.

8. **Customer Obligations.** Customer will be responsible for the following: (a) reporting errors promptly; (b) providing sufficient information for Ventiv to duplicate the circumstances of a reported Software defect or duplicate the error, as described in the Specifications, so Ventiv can duplicate the error, assess the situation, and/or undertake any needed or appropriate maintenance action hereunder; (c) designating two (2) members of its technical staff trained on the iVOS product to serve as Customer's sole representatives to contact Ventiv with maintenance issues ("**Customer's Support Contacts**"); and (d) carrying out procedures for the rectification of errors or malfunctions within a reasonable time after such procedures (or revisions, upgrades, enhancements, etc.) have been received from Ventiv.

9. **Helpdesk.** Ventiv provides services through its Helpdesk as set forth in the table below.

Support Type	Support Description	Expectation	Exclusions
Toll Free Live Phone Support	Hours available for live phone support	Monday - Friday 8:00am – 9:00 pm EST (US)	Ventiv Holidays
Emergency after-hours Support	Emergency after normal Business Hours on-call support	24x7x365	

	(24 hours a day, 7 days a week - Severity 1 issues only)		
Self-Service Portal	Online access to ticketing system to report an incident.	Response will be end of next Business Day	Use live or emergency for Severity 1

P1 = 24 x 7 through Ventiv support toll free telephone number: 1-800-980-9460
P2 = 24 hours per day during the five (5) business days (Monday through Friday), excluding Ventiv holidays.
P3 = During standard business hours (8:00 am to 9:00 pm) during the five (5) business days (Monday through Friday), excluding Ventiv holidays.
P4 = Monday through Friday by region (North America, APAC and EMEA) during standard business hours (8:00 am to 9:00 pm), excluding Ventiv holidays.

10. Proactive Support. Ventiv provides the following proactive support set forth in the table below.

Support Type	Support Description	Quarterly	Monthly	Weekly
Self-Service Portal	Online access to ticketing system to monitor status of outstanding tickets	✓	✓	✓
System Health Check	Regular scheduled health check of environment	✓	✓	✓
Account Review	Regular meeting with Account Management Team to review overall status including outstanding tickets and usage reports.	✓		
KPI Performance Report	System Key Performance Indicator report.		✓	

11. Incident Response for Functionality of the Software. The Software is designed and configured to meet minimal functionality standards as described in the Documentation and the Statement of Work. The following table illustrates the response level and resolution goal for loss of functionality of the Software.

Severity Classification	Severity Description	Initial Response Time	Follow-up Frequency	Resolution Goal
P1 - Critical	• Ventiv Software is completely inaccessible, or the majority of its critical functionality is unusable and no work around exists.	30 minutes during Business Hours	Every 60 minutes during Business Hours. After hours, update frequency will be mutually agreed upon.	8 Business Hours
P2 - Major	• One or more key features of Ventiv Software is unusable and no work around exists.	60 minutes during Business Hours	One Daily Update sent during Business Hours.	5 Business Days or by next scheduled maintenance window; whichever is less
P3 - Minor	• Non-critical functionality is down or impaired • Does not have significant current production impact • Performance is degraded	1 Business Day	As Agreed	As Agreed
P4 - General Request	• How to, training items, requests for general information • Enhancement requests	5 Business Days	As Agreed	As Agreed

12. **Customer Obligations.** Customer must make at least one of its two Customer Support Contacts available to work with the assigned Ventiv support resource(s) for all P1 and P2 issues. If Customer's Support Contacts are unavailable to work with Ventiv, then the issue will be lowered to a P3 issue. If an issue is considered P1, customer must call the Helpdesk

13. **Defect Resolution.** Should Ventiv, in its sole judgment, determine that there is a defect in the Software, it will, at its sole discretion, repair such defect in the version of the Software that Customer is currently using or instruct Customer to install a newer version of the Software with such defect repaired. Ventiv reserves the right to provide Customer with a work around in lieu of fixing a defect should it, in its sole judgment, determine that it is more effective to do so.

14. **Escalation Levels.**

Escalation Level	Contact Notified
State 1	Front-Line Support Manager
State 2	Global Support Services Director
State 3	VP Customer Management / Managing Director

Severity	Support State Levels	Escalation within the following time frames
P1 - Critical	State 1	1 Business Hour
	State 2	2 Business Hours
	State 3	8 Business Hours
P2 – Major	State 1	4 Business Hours
	State 2	8 Business Hours
	State 3	12 Business Hours
P3 – Minor	State 1	When agreed resolution time is not met.
P4 – General Request	All	N/A

15. **Maintenance Windows.** Ventiv will conduct regular weekly maintenance. The standard maintenance window will be six (6) hours in length. In the event that the required maintenance will require an extension, Ventiv will provide a written notice at least ten (10) Business Days in advance. Such extension will not exceed fifteen (15) total hours per week and all reasonable efforts will be taken for such extensions not to occur more than once in a five (5) week period. Ventiv will communicate directly with Customer on any maintenance specific to any dedicated resources.

Standard Maintenance Window:
ATLANTA Time: Friday 23:00– Saturday 05:00

Extended Maintenance Window:
ATLANTA Time: Friday 21:00 – Saturday 12:00

16. **Incident Response for Hosting Environment.** Ventiv provides proactive monitoring of the Hosting Environment. The Ventiv IT Operations staff is automatically notified by the monitoring systems within ten (10) minutes of an incident occurring that causes a material disruption, material performance degradation or outage to the Hosting Environment. The Ventiv customer support team will coordinate resolution and communication (status updates) with the Ventiv IT Operations staff and the Customer. Ventiv IT Operations will respond to issues with the Hosting Environment based on the severity levels defined below.

Severity Classification	Severity Description	Response Time	Follow-up Frequency	Resolution Goal	Monthly Metric
P1	Total inability to use any material part of the Hosting Environment, resulting in a critical impact on user objectives.	30 Minutes	Every 60 minutes during Business Hours; after	8 Business Hours	95% closed within resolution goal

Severity Classification	Severity Description	Response Time	Follow-up Frequency	Resolution Goal	Monthly Metric
			hours, update frequency will be mutually agreed upon.		
P2	Ability to use Hosting Environment, but user operation is severely restricted or where users notice degraded system performance.	1 hour	One Daily Update sent during Business Hours.	5 Business Days or by next scheduled maintenance window; whichever is less	90% closed within resolution goal
P3	Ability to use the Hosting Environment with minor faults that cause little disruption to service or use of the product. Failure relates to functions that are not critical to overall user operations.	1 Business Day	Every 2 days	5 Business Days or as agreed	90% closed within resolution goal

17. **Software Availability Service Level.** The Software will be available (as calculated below) to Customer ninety-nine percent (99%) of the time, twenty-four (24) hours per day, seven (7) days per week (a week will be deemed to commence at midnight Eastern Time on Sunday and extend for seven (7) days), including all legal holidays, with the exception of scheduled interruptions for maintenance and time required for deployment of vendor security patches or downtime resulting from general virus or denial of service attacks.

$$\text{Availability \%} = \frac{\text{Total Minutes minus Scheduled Downtime minus Unscheduled Downtime of the Software}}{\text{Total Minutes minus Scheduled Downtime of the Software}}$$

18. **Disaster Recovery Service Levels.**

Objective	Metric
Recovery Declaration	< 12 hours
RTO	< 24 hours
RPO	< 12 hours

19. **Hosting Environment Service Levels.**

Objective	Metric
Vulnerability Management	Weekly Vulnerability Scans and review of hosting and applications
Penetration Testing	Quarterly Penetration hosting and application testing performed by trusted independent third party
Uptime	99%, 24x7x365 except as detailed above
Calculation	$\% = \frac{\text{Total Minutes minus Scheduled Downtime minus Unscheduled Downtime}}{\text{Total Minutes minus Scheduled Downtime of the Hosting Environment}}$
Monitoring	24x7x365
Redundancy	Maintain redundant or high availability infrastructure for production environment
Control Audit	Maintain a minimum of a SAS70 Type II or AICPA current standard process control certification

20. **Managed Services.**

20.1 Description. Customer will receive the number of hours of Managed Service Hours specified in Schedule B of this Agreement (Order Form) on an annual basis subject to payment of the Managed Service Hour Fees for the Software set forth in Schedule B in exchange for Ventiv providing the Managed Servicesas detailed below. "Managed Services" are services provided to Customer through a Client

Delivery Leadat a higher level than Customer Support Services and provides overall consultancy for training, understanding the Customer's business process and how any change may impact other areas of the System. The Client Delivery Lead also act as Customer's advocate in product enhancements and providing periodic updates to the client via open items calls, account status reports and stewardship meetings conducted via Webex. Client Delivery Leads provide customers with the additional support as customers become familiar with the System. The Client Delivery Lead provides training and support through the implementation as new modules or users are added to the System. The Helpdesk is used for questions about the System operation, problems and enhancement requests.

20.2 How Managed Service Hours are Eroded. Ventiv enters all Customer Support Services and Managed Service into an online CRM. Any Customer Support Services provided to Customers to resolve errors in the Software that are not Customer-Created Errors, will not result in depletion of any Managed Service Hours purchased by Customer. During the implementation, the Client Delivery Lead is introduced to Customer and participates in the implementation. Once the implementation has been completed (and/or Customer requests changes to existing functionality that had previously been agreed), Managed Service Hours are eroded for changes to the System, such as adding or removing fields, adding rules, adding validations, etc. When the requested changes are for the purpose of adding a new module or a full business process, the Client Delivery Lead will identify that the suggested work is new scope and will be completed via an amendment to the Agreement at additional time and expense.

20.3 Tracking Managed Service Hours. Ventiv will maintain a database of Managed Service Hours used by Customer and will update this database within two weeks following the end of each calendar month. Once the appropriate time entries have been made, Ventiv will make this information available to Customer. Customer will have 30 days from the time this information is made available to dispute the validity of the entries. Should this occur Customer should state in writing to their Ventiv Client Delivery Lead, that the hours utilized are being contested and the reason for the dispute. At that time, Customer and its services manager will negotiate a reasonable resolution. Should the annually budgeted number of hours be exceeded, Ventiv will provide an invoice for the number of excess hours used at the hourly rate listed in Section VII.G. (Additional Fees) of Schedule B along with supporting documentation, on a quarterly basis.

EXHIBIT B

ATTACHMENT 1 - STATEMENT OF WORK (IVOS, RISK CONSOLE ADVANCE, CAPTURE)

This Attachment 1 – Statement of Work ("SOW") includes a description of the Services to be performed during implementation of the Software, including without limitation, (i) Project Management – managing the project delivery; (ii) Business Analysis – requirements gathering, creating specifications, QA testing; (iii) Configuration – setup of Customer database including custom fields and custom business rules; (iv) Data Conversion – converting source data into format used by the Software; (v) Reporting – deploying standard templates, completing custom report development, as applicable, (vi) Training – training for Customer testing and go-live.

The Software that Ventiv is configuring for the Customer under this SOW is Ventiv's proprietary Risk Management Information System (RMIS) called ***RiskConsole Advance®.*** A description of each of the modules included within the Software being licensed to Customer is set forth in Schedule A to the Agreement to which this Attachment 1 relates.

The following outlines the Implementation Services as defined to date.

I. IMPLEMENTATION

A. RiskConsole Advance Implementation (Advanced Safety Solution):

Estimated Hours: 321 hours

This is a time & materials agreement, and as such, the estimate provided herein are based on the information that Ventiv has received to date. Ventiv has derived this estimate in good faith and will target providing the deliverables herein within such estimate(s). All projects will be monitored by Ventiv, and any overage forecasts will be provided to the Customer early and often in the project lifecycle. If the project is expected to have hours overage, Customer redefines the scope of services, or Customer provides new details in respect to such project, a change control document will be executed with the Customer for additional services before Ventiv incurs the additional services. Ventiv will bill said additional services at current rates.

- Configuration for the following modules in RiskConsole Advance:
  - Claims Management
  - Action Item
  - Root Cause
  - Meetings
  - Investigations

Configuration specifications will be completed by Ventiv outlining the changes required for each module based on the requirements meetings

- Project Management Services

- Data Conversion Services – Legacy Data

Module	Data Received From	File Type	Data Load Type
Safety Meetings	City of Denver	Excel/csv	Snapshot

- Data Conversion Services – Production Data (One Time and Ongoing Processing)

Module	Data Received From	File Type	Frequency	Data Load Type
Organization	iVOS	Standard	Daily	Snapshot
Claims / Incidents	iVOS	Standard	Daily	Transactional

NOTES:

- ❑ Refer to the Data Services section regarding the layout and format of the data provided to Ventiv.
- ❑ Charges assessed by any Third Party for the extract and delivery of data noted above are the responsibility of Customer. Ventiv fees do not include any fees assessed by any Third Party.
- ❑ Delivery of data from a Third Party is based on the schedule defined by the Third Party. Any changes to the Third Party's defined delivery schedule must be negotiated by Customer with the Third Party.
- ❑ A snapshot claim load is a summary load of claims data. Each claim is loaded with one amount for paid, incurred, and outstanding by financial bucket. No payment detail such as check number or payee information is included.
- ❑ Transactional load of claims data loads all transactions for paid, incurred, and outstanding, depending on what is provided by the source. Payment detail such as check number and payee is included. This allows for historical loss development to be created during the conversion.

- Deploy the standard report templates for all standard contracted modules noted above

- Assist with the Client Testing process

- Provide training
  - One (1) days of training for up to six (8) persons for Customer users at one location

- Global Services
  - One Currency
  - Base Currency – USD

B. iVOS and Capture Implementation:

Estimated Hours: 1410 hours

This is a time & materials agreement, and as such, the estimate provided herein are based on the information that Ventiv has received to date. Ventiv has derived this estimate in good faith and will target providing the deliverables herein within such estimate(s). All projects will be monitored by Ventiv, and any overage forecasts will be provided to the Customer early and often in the project lifecycle. If the project is expected to have hours overage, Customer redefines the scope of services, or Customer provides new details in respect to such project, a change control document will be executed with the Customer for additional services before Ventiv incurs the additional services. Ventiv will bill said additional services at current rates.

- Delivery of the following modules in iVOS:
  - Worker's Compensation Module
  - Liability Module
  - Document Imaging Module
  - 3rd Party Bill Review Interface
  - Employee Interface
  - Accounts Payable Interface
  - CMS Module
  - EDI FROI
  - EDI SROI

- Delivery of the following in Capture
  - 5 Intake Forms

- iVOS Data Conversion Services – Legacy Data

Module	Data Received From	File Type	Frequency	Data Load Type
Insured Policy Data	CS Stars	Database (Oracle) or ASCII Format	Worker's Compensation Liability	New Implementation
Core Claim Data	CS Stars	Database (Oracle) or ASCII Format	Worker's Compensation Liability	New Implementation
Financial Data	CS Stars	Database (Oracle) or ASCII Format	Worker's Compensation Liability	New Implementation
Contacts, Diaries, Notepad, Litigation, Vehicle, EDI, Work Status, and associated reference tables	CS Stars	Database (Oracle) or ASCII Format	Worker's Compensation Liability	New Implementation
Document Images	CS Stars	Database (Oracle) or ASCII Format	Worker's Compensation Liability	New Implementation
Document Images – Medical Records	SharePoint	Database (Oracle) or ASCII Format	Worker's Compensation Liability	New Implementation

NOTES:
- ❑ Refer to the Data Services section regarding the layout and format of the data provided to Ventiv.
- ❑ Charges assessed by any Third Party for the extract and delivery of data noted above are the responsibility of Customer. Ventiv fees do not include any fees assessed by any Third Party.
- ❑ Delivery of data from a Third Party is based on the schedule defined by the Third Party. Any changes to the Third Party's defined delivery schedule must be negotiated by Customer with the Third Party.

- Deploy the standard report templates for all standard contracted modules noted above

- Assist with the Client Testing process

- Provide training

- **Training** (Based on 6 total days of training)
  - System Overview Training - 16 attendees/class max
    - 1 training day
  - General User Training - 16 attendees/class max.
    - 2 training days
  - Reporter Training - 16 attendees/class max.
    - 2 training days
  - System Administrator - 16 attendees/class max.
    - 1 training day

- Global Services
  - One Currency
  - Base Currency – USD

II. PROJECT DELIVERABLES

A. RiskConsole Advance Deliverables (Advanced Safety Solution)

Organizational Hierarchy

Customer will be using an Organizational Hierarchy structure for its contracted modules as noted above.

- ❑ Hierarchy will be loaded from iVOS.
- ❑ Changes required to the Organization screen will be charged to the contracted implementation hours. A specification will be completed outlining the requested changes. The specification will be reviewed with Customer and will require signoff by Customer prior to work commencing.
- ❑ RiskConsole Advance supports multiple hierarchy structures (geographical, functional, etc.). However, creation of additional hierarchy structures is excluded from the scope.

Claims Management Module

- ❑ Standard Configuration will be offered to Customer. Changes required to the Claim screen will be charged to the contracted implementation hours.

- ❑ Standard coverages will include: Workers Compensation, Auto Liability, General Liability, Property, and Auto Physical Damage. Additional configuration for specialized coverages (Product Liability, Professional Liability, D&O, etc.) not previously identified will be charged to the contracted implementation hours.

Action Items Module

- ❑ Standard Configuration for the Action Items Module will be offered to Customer. Changes required to the screens will be charged to the contracted implementation hours.
- ❑ Each record will be unique with a unique identifier.

Root Cause Analysis Module

- ❑ Standard Configuration for the Root Cause Module will be offered to Customer. Changes required to the screens will be charged to the contracted implementation hours.
- ❑ Each record will be unique with a unique identifier.

Investigation Module

- ❑ Standard Configuration for the Investigation Module will be offered to Customer. Changes required to the Module will be charged to the contracted implementation hours.
- ❑ Ventiv will not load data into this module. Customer may use the Spreadsheet Import or Spreadsheet Update functionality to load or update the data information into RiskConsole.

Meetings Module

- ❑ Standard Configuration for the Meetings Module will be offered to Customer. Changes required to the Module will be charged to the contracted implementation hours.
- ❑ Loaded meeting information will not be linked to other records. Customer may manually link a meeting record to other records, i.e. organization, claim, property, etc. where required.

Data Services

Ventiv will provide the data conversion and data load services to Customer as outlined above.

Requirements:

- ❑ Data request letters must be completed by Customer and sent to all Third Parties from which data will be received by Ventiv for Customer. A copy of the letter must be provided to Ventiv to allow for preparation for receiving the file.
- ❑ Control totals must be provided by Third Party for all data feeds.
- ❑ All data must be provided in ASCII format.
- ❑ All data received from a Data Supplier or a Third Party must be encrypted and electronically transferred to the RiskConsole Advance ftp server or transferred using secure SFTP protocol.
- ❑ Data is not allowed to be transferred to Ventiv via email.
- ❑ If the required data is in an Excel spreadsheet, all data must be compiled onto one worksheet and saved as a CSV file before providing the file to Ventiv.
- ❑ Any changes to the configured layout of data loads in production will result in additional fees.
- ❑ One (1) initial data conversion is included during the implementation unless a specific number of refreshes are noted above. Any additional data conversions completed after the initial conversion during the implementation stage, will be charged separately on a per load charge.
- ❑ Customer is responsible for all data charges from all Third Parties.

Assumptions:

- ❑ Ventiv is not responsible for incorrect coding on the data from Third Parties.
- ❑ Customer or Third-Party data providers are responsible for delivering data to RiskConsole Advance via the secure mechanisms described above.
- ❑ Customer will be responsible for maintaining and verifying the integrity of any data where the source is a client system or database.

- ❑ The standard data reconciliation will be completed for the initial claim financial conversion for each data source. This includes Total claim count, Total Incurred, Total Paid, Total Outstanding and Total Recovery by coverage from the source control totals as compared to the RiskConsole Advance database. Any time required to complete a custom reconciliation will be charged to the contracted implementation hours.

Reports

Ventiv will deploy the standard report templates for the contracted modules. Standard reports are accessible through a Business Intelligence link that appears under the Reporting menu option. Users may run the standard report templates ad-hoc or create 'report views' off these templates and run the report views on a recurring basis via scheduling. Many report views can be created off a single report template with each report view given a unique name that reflects the user's saved filter criteria.

Exclusions from Scope

Any requirement not specifically stated as included within this scope statement is considered outside the scope of the project.

B. iVOS Deliverables

- Configuration for iVOS Claims Management

Configuration of the iVOS claims module will be the primary responsibility of Customer. Ventiv Project Management, Business Analysts and Trainers will provide the necessary instruction to complete this task. Configuration tasks are outlined below for Project Management/Implementation support to implement the following modules:

Workers Compensation Module

- The following jurisdictions purchased by Customer will be included with the implementation:
  - Colorado
- Standard Ventiv implementation includes loading of compensation rates for jurisdictions listed above and loading of all jurisdictional forms and reports. Review of forms and reports is the responsibility of Customer, and modification of correspondence variables (pre-filled values on state forms), is the task of Customer.
- Ventiv will provide standard compensation rates for the jurisdictions listed above. Review of jurisdictional compensation rates is the responsibility of Customer.
- Ventiv assistance with the initial EDI Setup and configuration is included for one (1) jurisdiction. This includes working with Customer to explain how to configure the system to produce FROI and SROI files, how to link rename jobs, encryption jobs, and ftp transfer jobs. In addition Ventiv will work with Customer to contact the jurisdiction to determine the testing process.
- Customer will be responsible for creating and maintaining all security groups and roles, as well as the security on each tab within the application. This includes default values, read-only access, disabled and visibility properties, tooltips, restricted values and more. Implementation services will assist Customer in obtaining training and providing guidance in best practices with security.
- Ventiv will assist Customer with setting up reserve transaction codes, payment transaction codes, Customer insurance types and policy coverage information. Customer is responsible for providing the necessary information regarding Fiscal Year structure, Policy structure, Organization structure, and all other coded fields. Ventiv will provide best practice consulting on code configuration and maintenance. Customer is responsible for reviewing and confirming the reserve transactions have been setup correctly. Any reserve or payment mapping changes identified after Trial 1 conversion has been delivered to Customer will incur additional costs not included in this Statement of Work.

Liability Module

- The Liability Module allows for tracking of claims for all liability lines of business. Customer has contracted for the following lines of business:
  - General Liability
  - Auto Liability
  - Property Liability

- Customer will be responsible for creating and maintaining all security groups and roles, as well as the security on each tab within the application. This includes, default values, read-only access, disabled and visibility properties, tooltips, restricted values and more. Implementation services will assist Customer in obtaining training and providing guidance in best practices with security.
- Ventiv will assist Customer with setting up insurance types, reserve transaction codes, payment transaction codes, Customer insurance types and policy coverage information. Customer is responsible for providing the necessary information regarding Fiscal Year structure, Policy structure, Organization structure, and all other coded fields. Ventiv will provide best practice consulting on code configuration and maintenance. Customer is responsible for reviewing and confirming the reserve transactions have been setup correctly. Any reserve or payment mapping changes identified after Trial 1 conversion has been delivered to Customer will incur additional costs not included in this Statement of Work.

Reporter Module (includes Report Design and Distribution Tools)

- Ventiv will deliver all standard templates with application.
- Ventiv will configure the following reports as part of the standard implementation: Claim Log, Claim Summary, Payment Total, Reserve Total, and a severity report of Customer's choosing.
- Ventiv will also schedule one report within Scheduler and provide one Distribution Item as an example for Customer.
- Ventiv will provide training on Reporter and Report Designer, as well as Scheduler and Distribution.
- Customer is fully responsible for configuring, maintaining and customizing all reports. In addition, all scheduling of reports and distribution of the reports is the responsibility of Customer.

Business Rules

- Ventiv will provide all iVOS Business Rule templates with the iVOS application.

iVOS Scheduler

- Ventiv will deliver Scheduler with the iVOS application.
- Ventiv will setup and configure one set of batch jobs that are part of this implementation effort. Ventiv will setup and configure payment processing jobs. Ventiv will work with Customer when configuring jobs to ensure that the following examples of parameters are accurate: filenames, paths, timing, links, and all other definable attributes. Ventiv will provide a review of all scheduled jobs defined by Ventiv prior to go live.
- Customer is responsible for the setup and maintenance of any duplicative jobs (for example Ventiv will setup the, subsequent states will be the responsibility of Customer) as well as have a clear understanding of all jobs set in scheduler.

Document Imaging

- Enables the attachment of scanned documents to iVOS claim records. The iVOS imaging workflow is highly configurable and can be tailored specifically to handle a Customer's interface/integration requirements. iVOS can be configured to save images either in the claims database, or in a file structure.
- Ventiv will configure the standard module.

Employee Interface

- iVOS has a standard employee import interface (fixed-width flat file). When a claim (or injury report) is opened and a Social Security or employee number is entered, the employee information is automatically populated into the general claim window, eliminating the need to manually enter the data.
- Ventiv will configure the standard module.

Third Party Interface – Bill Review

- A fixed-width flat file that imports and exports bill review information. Claim and Vendor information is exported from iVOS and Payment and Fee information is imported into iVOS.
- Ventiv will configure the standard module.

CMS Module

- Includes several iVOS scheduled jobs and business rules for processing the mandatory claims data to meet Section III reporting requirements. Features include assigning/managing Responsible Reporting Entity (RRE) IDs, running data validation reports, generating export files, importing CMS responses, and updating claims, as well us notifying adjusters of data validation issues and claim updates.
- Ventiv will configure the standard module.

EDI FROI

- iVOS includes a standard interface to support all state-mandated workers' compensation EDI, and fully supports IAIABC Release 1, 2 and 3 transmission requirements. The interface will produce an export file that contains data formatted for transmission to the appropriate jurisdiction.
- Ventiv will configure the standard module for the purchased jurisdiction in Schedule B.

EDI SROI

- Supports all requirements for mandated EDI reporting of the Subsequent Report of Injury (SROI). The interface will produce an export that contains data formatted for transmission to the appropriate jurisdiction. Specific states are indicated in the Order Form in Schedule B.
- Ventiv will configure the standard module for the purchased jurisdiction in Schedule B.

Accounts Payable Interface

- This is a two way interface with payment and payee into formation extracted from iVOS. Check date, check number and payment id returned to the customer. Customer is responsible for providing necessary requirements for the outbound extract file. Extract file must be fixed length flat file. Ventiv will develop the outbound layout to meet the requirements. Inbound file should be a fixed length flat file with the iVOS payment id as well as the check date and check number. Standard security protocols must be adhered to. Implementation hours do not include support for customer's development team.

Data Conversion Services

- Standard iVOS Claim Conversions include the following conversion phases and should include a minimum of 2 Trials prior to the Go Live conversion: Each conversion must include Policy data, core Claim data, financial data and Contacts/Diaries/Notepads, etc. as noted in Schedule B.
- For each module in Schedule B, the following outlines a list of the sub-modules to be converted as part of the iVOS standard Claims conversion.
- Insured Policy Data includes the conversion of Users, Examiners, Policy Information (includes basic coverage and policy periods), Fiscal Year setup, Organization, Insured and Insurers.
- Core Claim Data includes claim, claimant, employment, work comp claimant, claim indicators and associated reference tables such as claimant type, incident type, body part, claim cause, nature of injury, class codes, occupation, incident location, adjusting office, work comp claimant associated reference tables, etc.
- Financial Data includes vendor, payee, reserve history, payment transaction history, payment check, and associated reference tables such as reserve categories, payment transaction codes and reserve reasons

NOTE: Charges assessed by a Third Party for the extract and delivery of data noted above is the responsibility of Customer. Ventiv fees do not include fees assessed by a Third Party. Delivery of data from a Third Party is based on the schedule defined by the Third Party. All changes to the Third Party's defined delivery schedule must be negotiated by Customer with the Third Party.

Requirements:

- Data request letters must be completed by Customer and sent to all Third Parties from which data will be received by Ventiv for Customer. A copy of the letter must be provided to Ventiv to allow for preparation for receiving the file.
- Customer extraction and delivery of data and financial balancing reports is a successfully tested repeatable process.
- Customer will provide all tables and/or files from their source system that contain data, including reference and transactional, to be converted into iVOS.
- Ventiv requires that all data, including that from a Data Supplier or a Third Party, is encrypted and received via secured ftp (sFTP). An encrypted hard drive is an acceptable alternative.
- Data is not allowed to be transferred to Ventiv via email or unencrypted to an unsecured ftp (FTP) site.
- All data must be provided in one of the following accepted data formats:
  - Oracle schema
  - SQLServer database
  - MS Access database
  - Fixed length, unpacked, ASCII text file (file layouts required)
  - Delimited, unpacked ASCII text file (file layouts required)
- Any changes to the source data layout after Trial 1 Customer sign-off will follow Ventiv's standard change management process.
- A data dictionary and/or ERD will be provided by the Customer or a Third Party, on behalf of the Customer. If no data dictionary is available, access to a person with in depth knowledge of the database must be provided.
- Financial balancing information is provided by the Customer or a Third Party, on behalf of the Customer. The reports are generated from the delivered source data, contain the following information, and are delivered with every delivery of source data.
  - Total Claim counts, summarized by open and closed
  - Paid amounts
  - Total Incurred and/or outstanding Reserves
  - Recovery amounts
- Financial balancing reports are expected to provide detail that is summarized by:
  - Fiscal Year
  - Insured/Org Structure
  - Claim level detail
- The following tasks need to be performed by the customer for the trial and final conversions:
  - Financial Balancing Validation
  - Data Conversion Mapping Validation
  - Application Functionality Validation
- Additions to Line(s) of Business will follow Ventiv's standard change management process.
- Functional data outside the above list of tables will follow Ventiv's standard change management process.
- Custom conversion into Client Defined Columns will follow Ventiv's standard change management process.
- Additional fees are required for creation of filters needed to segregate specific claims for conversion to iVOS from delivered source.
- Additional fees are required for converting into notepads as a plain text notepad body from a source that is not plain text, such as HTML, XML, MSWord, etc.

- For Document Image conversions:
  - Ventiv is not responsible for extraction of document image files from a Third Party system.
  - Ventiv is not responsible for renaming extracted document image files to produce unique file names.
  - All document image files should be provided in a single root directory.
  - Additional fees are required to manipulate document image file names or directory structures differing from standard Ventiv hosted environment requirements.
- All reference table codes/descriptions must be defined by Customer (ex: injury codes, body part codes, payment codes etc.)
- Complete reference table mappings from source code values to iVOS code values are to be provided by the Customer where mappings are required.

- All conversion development and conversion program unit testing is completed within the Ventiv environment.
- The Customer's signoff is required after completion of mapping source data fields to iVOS fields and prior to the start of conversion development.
- The Customer's signoff is required on each trial conversion and the final conversion and indicates the Customer's validation and acceptance of converted data and mapping transformations.

Assumptions:

- Customer is responsible for data after export jobs complete. After export is complete, Customer can use or route this file to their specific need.
- Data conversions for new implementations will be completed on the latest General Released version of the iVOS application.
- Ventiv will provide the Conversion reconciliation report, mapping and transformation documentation to the Customer.
- The standard data reconciliation will be completed for the claim financial conversion. This includes total claim count, total incurred, total paid, total outstanding and total recoveries by fiscal year from the source Financial Balancing reports as compared to the iVOS database. Any time required to develop and validate a custom reconciliation will be charged to the project by standard rates specified in the Statement of Work.
- Ventiv will transfer the standard security and configuration setup from the Customer test environment to the applicable Conversion database per a defined set of standard iVOS configuration tables. The list of tables will be delivered to Customer as part of the project planning exercise. The Customer is responsible for validating functionality after this transfer of data.

IV. GENERAL ASSUMPTIONS

- ❑ Cost estimates based on an anticipated total record count of up to **250** gigabytes of storage plus 75 gigabytes of attachments during the proposed contract period.
- ❑ The standard file attachment size is limited to 5 megabytes per attachment. Upon request, the file attachment size may be increased to 10 megabytes per attachment.
- ❑ Customer Project Manager will be responsible for managing the project and obtaining consensus and sign-off on requirements and work products.
- ❑ Customer will be responsible for engaging all client stakeholders and facilitating / organizing all internal client relationships to allow full mobilization of a project team with support from the Ventiv Project Manager.
- ❑ Customer will dedicate sufficiently skilled resources to support the Services as described within this Statement of Work.
- ❑ Customer will provide the requested resources, with the requested skills and project dedication as outlined in a mutually agreed upon work plan.
- ❑ Customer will identify resource(s) to transition to and take ownership of the project deliverables.
- ❑ Customer will be responsible for providing internal change management, communications planning, and internal marketing for any project.
- ❑ Any critical code changes that must be implemented in any client systems that affect data provided to RiskConsole Advance will be reviewed by Ventiv to determine the impact, if any, on fees and timeline for the implementation.

Client Testing

DURING THE IMPLEMENTATION, VENTIV WILL REQUIRE CLIENT TESTING ON EACH PROJECT DELIVERABLE AS VENTIV DEPLOYS SUCH DELIVERABLE TO CUSTOMER. CLIENT TESTING TIMELINES WILL BE OUTLINED IN THE PROJECT PLAN TO BE COMPLETED AFTER THE PROJECT KICKOFF. CUSTOMER RESOURCES WILL BE TRAINED AND ARE REQUIRED TO COMPLETE CLIENT TESTING WITHIN THE AGREED TO TIMELINES. TIME REQUIRED TO COMPLETE CLIENT TESTING WILL VARY DEPENDING ON THE COMPLEXITY OF THE DELIVERABLE. VENTIV WILL OBTAIN SIGNOFF FROM CUSTOMER ON EACH DELIVERABLE AS CLIENT TESTING IS COMPLETED THROUGHOUT THE IMPLEMENTATION. IMPLIED SIGNOFF IS INCORPORATED FOR DELIVERABLE AND PROJECT SIGNOFF INDICATING THAT CUSTOMER MUST PROVIDE FEEDBACK ON ANY ISSUES WITHIN TEN (10) BUSINESS DAYS FROM RECEIPT OF THE SIGNOFF LETTER. IF FEEDBACK IS NOT RECEIVED WITHIN THE DEFINED TIME PERIOD, ACCEPTANCE OF THE DELIVERABLE AND/OR PROJECT IS ASSUMED.

Completion Criteria

- ❑ "Go Live Date" is when the deliverables of this Statement of Work have been deployed to production and made available for their intended use
- ❑ As an early step in implementation, Ventiv will work with Client to establish a target "Estimated Go Live Date". This may change through mutual collaboration as details are confirmed, particularly in the earlier part of the implementation
- ❑ Ventiv will request confirmation from Client that "Go Live Date" has been achieved. No response for 30 days will constitute implied confirmation
- ❑ If client wishes to have a material portion of this Statement of Work deployed to production and made available (i.e. partially "go live"), Ventiv may require the Statement of Work be split accordingly.
- ❑ "Transition Period" is the 30 days after Go Live Date during which time Ventiv services pertaining to this Statement of Work are considered part of the implementation. After the Transition Period, Ventiv services pertaining to this Statement of Work will be considered Managed Service Hours (see Ongoing Support section).

V. IDENTIFIED RISKS AND MITIGATION

Risk	Resolution
Customer key project personnel are not available, either due to personal or work commitments	Backup resources need to be available and up to speed to address gaps in resource capacity. Workloads of project personnel need to be adjusted to account for project requirements. Documentation must be logged in common area and accessible to all project team members.
User does not have connection to the internet	User will need to have internet installed at site. User workstation must meet minimum requirements for operating system, Internet Explorer and Internet connection.
Organizational hierarchy can't be	Conversion programs can be prepared and data first loaded into system with default location then

completed on schedule	updated on subsequent runs.
Third Party cannot send required data	Customer and Ventiv will need to determine how to load data, either manually or via external extracts from Third Party system, into RiskConsole Advance.
Poor quality data (invalid codes, unexpected records, missing records)	Analysis of data prior to loading to RiskConsole Advance to identify issues and get source to fix where possible. Establish exception reports to identify data problems during production.
Data anomalies discovered after reports have been developed.	Try to get source to correct data, if not, attempt to account for data anomaly during data load, and, finally, if all else fails, adjust reports to accommodate for data anomaly.
Data cannot be provided via encrypted transfer protocol	Ventiv to provide guidance around options for encryption software and ftp transfer.

EXHIBIT C

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY): 12/6/2018

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER Crystal & Company Crystal IBC LLC 32 Old Slip New York NY 10005	**CONTACT NAME:** Jamila Aziz **PHONE (A/C, No, Ext):** 800-221-5830 **FAX (A/C, No):** 800-383-1852 **E-MAIL ADDRESS:** Jamila.aziz@crystalco.com
INSURED VENTTE Ventiv Technology, Inc. 3350 Riverwood Parkway, Suite 2000 Atlanta GA 30339	**INSURER(S) AFFORDING COVERAGE** / **NAIC #** **INSURER A :** Valley Forge Insurance Company 20508 **INSURER B :** National Fire Insurance Company of Hart 20478 **INSURER C :** The Continental Insurance Company 35289 **INSURER D :** **INSURER E :** **INSURER F :**

COVERAGES **CERTIFICATE NUMBER:** 1330443627 **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	X **COMMERCIAL GENERAL LIABILITY** [ ] CLAIMS-MADE [X] OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: [X] POLICY [ ] PRO-JECT [ ] LOC [ ] OTHER:	Y	Y	6072449601	6/30/2018	6/30/2019	EACH OCCURRENCE DAMAGE TO RENTED PREMISES (Ea occurrence) MED EXP (Any one person) PERSONAL & ADV INJURY GENERAL AGGREGATE PRODUCTS - COMP/OP AGG	$ 1,000,000 $ 1,000,000 $ 15,000 $ 1,000,000 $ 2,000,000 $ 2,000,000
B	**AUTOMOBILE LIABILITY** [ ] ANY AUTO [ ] OWNED AUTOS ONLY [ ] SCHEDULED AUTOS [X] HIRED AUTOS ONLY [X] NON-OWNED AUTOS ONLY			6072449615	6/30/2018	6/30/2019	COMBINED SINGLE LIMIT (Ea accident) BODILY INJURY (Per person) BODILY INJURY (Per accident) PROPERTY DAMAGE (Per accident)	$ 1,000,000 $ $ $
C	X **UMBRELLA LIAB** X OCCUR **EXCESS LIAB** [ ] CLAIMS-MADE [ ] DED [X] RETENTION $ $10,000			6072449551	6/30/2018	6/30/2019	EACH OCCURRENCE AGGREGATE	$ 10,000,000 $ 10,000,000
C	**WORKERS COMPENSATION AND EMPLOYERS' LIABILITY** Y / N ANYPROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? [ ] **(Mandatory in NH)** If yes, describe under DESCRIPTION OF OPERATIONS below	N / A		6072449579	6/30/2018	6/30/2019	X PER STATUTE [ ] OTH-ER E.L. EACH ACCIDENT E.L. DISEASE - EA EMPLOYEE E.L. DISEASE - POLICY LIMIT	 $ 1,000,000 $ 1,000,000 $ 1,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

Risk Management Information System, 28659Q

As required by written contract, the City and County of Denver, its Elected and Appointed Officials, Employees and Volunteers are included as Additional Insured.

CERTIFICATE HOLDER

Risk Management Information System, 28659Q

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

Crystal & Company

EXHIBIT D

HIPAA/HITECH (Business Associate Terms)

1. GENERAL PROVISIONS AND RECITALS

1.01 The parties agree that the terms used, but not otherwise defined below, shall have the same meaning given to such terms under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("the HITECH Act"), and their implementing regulations at 45 CFR Parts 160 and 164 ("the HIPAA regulations") as they exist or may hereafter be amended.

1.02 The parties agree that a business associate relationship (as described in 45 CFR §160.103) under HIPAA, the HITECH Act, and the HIPAA regulations arises between the CONTRACTOR and the CITY to the extent that CONTRACTOR performs, or delegates to subcontractors to perform, functions or activities on behalf of CITY.

1.03 CITY wishes to disclose to CONTRACTOR certain information, some of which may constitute Protected Health Information ("PHI") as defined below, to be used or disclosed in the course of providing services and activities.

1.04 The parties intend to protect the privacy and provide for the security of PHI that may be created, received, maintained, transmitted, used, or disclosed pursuant to the Agreement in compliance with the applicable standards, implementation specifications, and requirements of HIPAA, the HITECH Act, and the HIPAA regulations as they exist or may hereafter be amended.

1.05 The parties understand and acknowledge that HIPAA, the HITECH Act, and the HIPAA regulations do not pre-empt any state statutes, rules, or regulations that impose more stringent requirements with respect to privacy of PHI.

1.06 The parties understand that the HIPAA Privacy and Security rules apply to the CONTRACTOR in the same manner as they apply to a covered entity. CONTRACTOR agrees to comply at all times with the terms of this Agreement and the applicable standards, implementation specifications, and requirements of the Privacy and the Security rules, as they exist or may hereafter be amended, with respect to PHI.

2. DEFINITIONS.

2.01 "Administrative Safeguards" are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic PHI and to manage the conduct of CONTRACTOR's workforce in relation to the protection of that information.

2.02 "Agreement" means the attached Agreement and its exhibits to which these additional terms are incorporated by reference.

2.03 "Breach" means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI.

2.03.1 Breach excludes:

1. any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of CONTRACTOR or CITY, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.

2. any inadvertent disclosure by a person who is authorized to access PHI to another person authorized to access PHI, or organized health care arrangement in which CITY participates, and the information received as a result of such disclosure is not further used or disclosed in a manner disallowed under the HIPAA Privacy Rule.

3. a disclosure of PHI where CONTRACTOR or CITY has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

2.03.2 Except as provided in paragraph (a) of this definition, an acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule is presumed to be a breach unless CONTRACTOR demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

b. The unauthorized person who used the PHI or to whom the disclosure was made;

c. Whether the PHI was actually acquired or viewed; and

d. The extent to which the risk to the PHI has been mitigated.

2.04 "CONTRACTOR" shall have the same meaning as in the attached Agreement, to which these Business Associate terms are incorporated by reference.

2.05 "CITY" shall have the same meaning as in the attached Agreement, to which these Business Associate terms are incorporated by reference.

2.06 "Data Aggregation" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR §164.501.

2.07 "Designated Record Set" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR §164.501.

2.08 "Disclosure" shall have the meaning given to such term under the HIPAA regulations in 45 CFR §160.103.

2.09 "Health Care Operations" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR §164.501.

2.10 "Immediately" where used here shall mean within 24 hours of discovery.

2.11 "Individual" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR §160.l03 and shall include a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).

2.12 "Parties" shall mean "CONTRACTOR" and "CITY", collectively.

2.13 "Physical Safeguards" are physical measures, policies, and procedures to protect CONTRACTOR's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

2.14 "The HIPAA Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.

2.15 "Protected Health Information" or "PHI" shall have the meaning given to such term under the HIPAA regulations at 45 CFR §160.103.

2.16 "Required by Law" shall have the meaning given to such term under the HIPAA Privacy Rule at 45 CFR §164.103.

2.17 "Secretary" shall mean the Secretary of the Department of Health and Human Services or his or her designee.

2.18 "Security Incident" means attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. "Security incident" does not include trivial incidents that occur on a daily basis, such as scans, "pings", or unsuccessful attempts to penetrate computer networks or servers maintained by CONTRACTOR.

2.19 "The HIPAA Security Rule" shall mean the Security Standards for the Protection of electronic PHI at 45 CFR Part 160, Part 162, and Part 164, Subparts A and C.

2.20 "Subcontractor" shall have the meaning given to such term under the HIPAA regulations at 45 CFR §160.103.

2.21 "Technical safeguards" means the technology and the policy and procedures for its use that protect electronic PHI and control access to it.

2.22 "Unsecured PHI" or "PHI that is unsecured" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of Health and Human Services ("HHS") in the guidance issued on the HHS Web site.

2.23 "Use" shall have the meaning given to such term under the HIPAA regulations at 45 CFR §160.103.

3. OBLIGATIONS AND ACTIVITIES OF CONTRACTOR AS BUSINESS ASSOCIATE.

3.01 CONTRACTOR agrees not to use or further disclose PHI that CITY discloses to CONTRACTOR except as permitted or required by this Agreement or by law.

3.02 CONTRACTOR agrees to use appropriate safeguards, as provided for in this Agreement, to prevent use or disclosure of PHI that CITY discloses to CONTRACTOR or that CONTRACTOR creates, receives, maintains, or transmits, on behalf of CITY, except as provided for by this Contract.

3.03 CONTRACTOR agrees to comply with the HIPAA Security Rule, at Subpart C of 45 CFR Part 164, with respect to electronic PHI that CITY discloses to CONTRACTOR or that CONTRACTOR creates, receives, maintains, or transmits, on behalf of CITY.

3.04 CONTRACTOR agrees to mitigate, to the extent practicable, any harmful effect of a Use or Disclosure of PHI by CONTRACTOR in violation of the requirements of this Agreement that becomes known to CONTRACTOR.

3.05 CONTRACTOR agrees to immediately report to CITY any Use or Disclosure of PHI not provided for by this Agreement that CONTRACTOR becomes aware of. CONTRACTOR must report Breaches of Unsecured PHI in accordance with 45 CFR §164.410.

3.06 CONTRACTOR agrees to ensure that any of its subcontractors that create, receive, maintain, or transmit, PHI on behalf of CONTRACTOR agree to comply with the applicable requirements of Section 164 Part C by entering into a contract or other arrangement.

3.07 To comply with the requirements of 45 CFR §164.524, CONTRACTOR agrees to provide access to CITY, or to an individual as directed by CITY, to PHI in a Designated Record Set within fifteen (15) calendar days of receipt of a written request by CITY.

3.08 CONTRACTOR agrees to make amendment(s) to PHI in a Designated Record Set that CITY directs or agrees to, pursuant to 45 CFR §164.526, at the request of CITY or an Individual, within thirty (30) calendar days of receipt of the request by CITY.

CONTRACTOR agrees to notify CITY in writing no later than ten (10) calendar days after the amendment is completed.

3.09 CONTRACTOR agrees to make internal practices, books, and records, including policies and procedures, relating to the use and disclosure of PHI received from, or created or received by CONTRACTOR on behalf of CITY, available to CITY and the Secretary in a time and manner as determined by CITY, or as designated by the Secretary, for purposes of the Secretary determining CITY'S compliance with the HIPAA Privacy Rule.

3.10 CONTRACTOR agrees to document any Disclosures of PHI that CITY discloses to CONTRACTOR or that CONTRACTOR creates, receives, maintains, or transmits on behalf of CITY, and to make information related to such Disclosures available as would be required for CITY to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 CFR §164.528.

3.11 CONTRACTOR agrees to provide CITY information in a time and manner to be determined by CITY in order to permit CITY to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 CFR §164.528.

3.12 CONTRACTOR agrees that, to the extent CONTRACTOR carries out CITY's obligation(s) under the HIPAA Privacy and/or Security rules, CONTRACTOR will comply with the requirements of 45 CFR Part 164 that apply to CITY in the performance of such obligation(s).

3.13 CONTRACTOR shall work with CITY upon notification by CONTRACTOR to CITY of a Breach to properly determine if any Breach exclusions exist as defined below.

4. SECURITY RULE.

4.01 CONTRACTOR shall comply with the requirements of 45 CFR § 164.306 and establish and maintain appropriate Administrative, Physical and Technical Safeguards in accordance with 45 CFR §164.308, §164.310, §164.312, §164.314 and §164.316 with respect to electronic PHI that CITY discloses to CONTRACTOR or that CONTRACTOR creates, receives, maintains, or transmits on behalf of CITY. CONTRACTOR shall follow generally accepted system security principles and the requirements of the HIPAA Security Rule pertaining to the security of electronic PHI.

4.02 CONTRACTOR shall ensure that any subcontractors that create, receive, maintain, or transmit electronic PHI on behalf of CONTRACTOR agree through a contract with CONTRACTOR to the same restrictions and requirements contained here.

4.03 CONTRACTOR shall immediately report to CITY any Security Incident of which it becomes aware. CONTRACTOR shall report Breaches of Unsecured PHI as described in 5. BREACH DISCOVERY AND NOTIFICATION below and as required by 45 CFR §164.410.

5. BREACH DISCOVERY AND NOTIFICATION.

5.01 Following the discovery of a Breach of Unsecured PHI, CONTRACTOR shall notify CITY of such Breach, however, both parties may agree to a delay in the notification if so advised by a law enforcement official pursuant to 45 CFR §164.412.

5.01.1 A Breach shall be treated as discovered by CONTRACTOR as of the first day on which such Breach is known to CONTRACTOR or, by exercising reasonable diligence, would have been known to CONTRACTOR.

5.01.2 CONTRACTOR shall be deemed to have knowledge of a Breach, if the Breach is known, or by exercising reasonable diligence would have been known, to any person who is an employee, officer, or other agent of CONTRACTOR, as determined by the federal common law of agency.

5.02 CONTRACTOR shall provide the notification of the Breach immediately to the CITY DEH Executive Director or other designee.

5.02.1 CONTRACTOR'S initial notification may be oral, but shall be followed by written notification within 24 hours of the oral notification.

5.03 CONTRACTOR'S notification shall include, to the extent possible:

5.03.l The identification of each Individual whose Unsecured PHI has been, or is reasonably believed by CONTRACTOR to have been, accessed, acquired, used, or disclosed during the Breach;

5.03.2 Any other information that CITY is required to include in the notification to each Individual under 45 CFR §164.404 (c) at the time CONTRACTOR is required to notify CITY, or promptly thereafter as this information becomes available, even after the regulatory sixty (60) day period set forth in 45 CFR §164.410 (b) has elapsed, including:

a. A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;

b. A description of the types of Unsecured PHI that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

c. Any steps Individuals should take to protect themselves from potential harm resulting from the Breach;

d. A brief description of what CONTRACTOR is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any future Breaches; and

e. Contact procedures for Individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

5.04 CITY may require CONTRACTOR to provide notice to the Individual as required in 45 CFR §164.404, if at the sole discretion of the CITY, it is reasonable to do so under the circumstances.

5.05 In the event that CONTRACTOR is responsible for a Breach of Unsecured PHI in violation of the HIPAA Privacy Rule, CONTRACTOR shall have the burden of demonstrating that CONTRACTOR made all required notifications to CITY, and as required by the Breach notification regulations, or, in the alternative, that the acquisition, access, use, or disclosure of PHI did not constitute a Breach.

5.06 CONTRACTOR shall maintain documentation of all required notifications of a Breach or its risk assessment under 45 CFR §164.402 to demonstrate that a Breach did not occur.

5.07 CONTRACTOR shall provide to CITY all specific and pertinent information about the Breach, including the information listed above, if not yet provided, to permit CITY to meet its notification obligations under Subpart D of 45 CFR Part 164 as soon as practicable, but in no event later than fifteen (15) calendar days after CONTRACTOR's initial report of the Breach to CITY.

5.08 CONTRACTOR shall continue to provide all additional pertinent information about the Breach to CITY as it becomes available, in reporting increments of five (5) business days after the prior report to CITY. CONTRACTOR shall also respond in good faith to all reasonable requests for further information, or follow-up information, after report to CITY, when such request is made by CITY.

5.09 In addition to the provisions in the body of the Agreement, CONTRACTOR shall also bear all expense or other costs associated with the Breach and shall reimburse CITY for all expenses CITY incurs in addressing the Breach and consequences thereof, including costs of investigation, notification, remediation, documentation or other costs or expenses associated with addressing the Breach.

6. PERMITTED USES AND DISCLOSURES BY CONTRACTOR.

6.01 CONTRACTOR may use or further disclose PHI that CITY discloses to CONTRACTOR as necessary to perform functions, activities, or services for, or on behalf of, CITY as specified in the Agreement, provided that such use or Disclosure would not violate the HIPAA Privacy Rule if done by CITY.

6.02 CONTRACTOR may use PHI that CITY discloses to CONTRACTOR, if necessary, for the proper management and administration of the Agreement.

6.03 CONTRACTOR may disclose PHI that CITY discloses to CONTRACTOR to carry out the legal responsibilities of CONTRACTOR, if:

6.03.1 The Disclosure is required by law; or

6.03.2 CONTRACTOR obtains reasonable assurances from the person or entity to whom/which the PHI is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person or entity and the person or entity immediately notifies CONTRACTOR of any instance of which it is aware in which the confidentiality of the information has been breached.

6.04 CONTRACTOR may use or further disclose PHI that CITY discloses to CONTRACTOR to provide Data Aggregation services relating to the Health Care Operations of CONTRACTOR.

6.05 CONTRACTOR may use and disclose PHI that CITY discloses to CONTRACTOR consistent with the minimum necessary policies and procedures of CITY.

7. OBLIGATIONS OF CITY.

7.01 CITY shall notify CONTRACTOR of any limitation(s) in CITY'S notice of privacy practices in accordance with 45 CFR §164.520, to the extent that such limitation may affect CONTRACTOR'S Use or Disclosure of PHI.

7.02 CITY shall notify CONTRACTOR of any changes in, or revocation of, the permission by an Individual to use or disclose his or her PHI, to the extent that such changes may affect CONTRACTOR'S Use or Disclosure of PHI.

7.03 CITY shall notify CONTRACTOR of any restriction to the Use or Disclosure of PHI that CITY has agreed to in accordance with 45 CFR §164.522, to the extent that such restriction may affect CONTRACTOR'S use or disclosure of PHI.

7.04 CITY shall not request CONTRACTOR to use or disclose PHI in any manner that would not be permissible under the HIPAA Privacy Rule if done by CITY.

8. BUSINESS ASSOCIATE TERMINATION.

8.01 Upon CITY'S knowledge of a material breach or violation by CONTRACTOR of the requirements of this Contract, CITY shall:

8.01.1 Provide an opportunity for CONTRACTOR to cure the material breach or end the violation within thirty (30) business days; or

8.01.2 Immediately terminate the Agreement, if CONTRACTOR is unwilling or unable to cure the material breach or end the violation within (30) days, provided termination of the Agreement is feasible.

8.02 Upon termination of the Agreement, CONTRACTOR shall either destroy or return to CITY all PHI CONTRACTOR received from CITY and any and all PHI that

CONTRACTOR created, maintained, or received on behalf of CITY in conformity with the HIPAA Privacy Rule.

8.02.1 This provision shall apply to all PHI that is in the possession of subcontractors or agents of CONTRACTOR.

8.02.2 CONTRACTOR shall retain no copies of the PHI.

8.02.3 In the event that CONTRACTOR determines that returning or destroying the PHI is not feasible, CONTRACTOR shall provide to CITY notification of the conditions that make return or destruction infeasible. Upon determination by CITY that return or destruction of PHI is infeasible, CONTRACTOR shall extend the protections of this Agreement to the PHI and limit further Uses and Disclosures of the PHI to those purposes that make the return or destruction infeasible, for as long as CONTRACTOR maintains the PHI.

8.03 The obligations of this Agreement shall survive the termination of the Agreement.