



**CONTRACT NUMBER MA-017-22010011**  
**BETWEEN**  
**THE COUNTY OF ORANGE**  
**AND**  
**RISKCONNECT, INC.**  
**FOR**  
**RISK AND CLAIMS MANAGEMENT INFORMATION SYSTEM SOLUTIONS**

This Contract **MA-017-22010011**, hereinafter referred to as “Contract”, is made and entered into upon execution of all necessary signatures between the County of Orange, hereinafter “County”, and Riskconnect, Inc., with a place of business at 1701 Barrett Lakes Blvd., NW, Ste 500, Kennesaw, GA 30144-4517, hereinafter referred to as “Contractor” or “Riskconnect”, which are sometimes individually referred to as “Party” or collectively referred to as “Parties”.

**ATTACHMENTS**

- Attachment A – Scope of Services  
Attachment A-1 – Additional Scope of Services  
Attachment B – Compensation/Cost  
Attachment C – Riskconnect Security and Service Levels  
Attachment D – HIPPA Business Associate Agreement  
Attachment E – Riskconnect Privacy Statement  
Attachment F – Supplemental Terms and Conditions (Riskconnect Applications)  
Attachment G – County’s User Provisioning Policy  
Attachment H - Data Classification Policy

**RECITALS**

**WHEREAS**, County desires to establish a Contract for Risk and Claims Management Information System Solutions, and

**WHEREAS**, Contractor agrees to provide Risk and Claims Management Information System Solutions as further set forth in Attachment A, Scope of Services, and Attachment A-1, Additional Scope of Services, attached hereto and incorporated herein; and

**WHEREAS**, Contractor agrees to accept the compensation as further set forth in Attachment B, Compensation/Cost, attached hereto and incorporated herein; and

**WHEREAS**, the County of Orange Board of Supervisors has authorized the Purchasing Agent or his designee to enter into a Contract to obtain a Risk and Claims Management Information System Solutions.

**NOW THEREFORE**, the Parties mutually agree as follows:

**ARTICLES**

**GENERAL TERMS AND CONDITIONS:**

- A. **Governing Law and Venue:** This Contract has been negotiated and executed in the State of California and shall be governed by and construed under the laws of the state of California, without reference to conflicts of laws provisions. In the event of any legal action to enforce or interpret this Contract, the sole and exclusive venue shall be a court of competent jurisdiction located in Orange County, California, and the Parties hereto agree to and do hereby submit to the jurisdiction of such court, notwithstanding Code of Civil Procedure section 394. Furthermore, the Parties specifically agree to waive any and all rights to request that an action be transferred for trial to another County.
- B. **Entire Contract:** This Contract, comprised of these terms and conditions and Attachments A, B, C, D, E, F, G, and H, which are incorporated herein and constitute part of this Contract, contains the entire contract between the Parties with respect to the matters herein and there are no restrictions, promises, warranties, or undertakings other than those set forth herein or referred to herein. No exceptions, alternatives,

substitutions, revisions, understandings, agreements, restrictions, promises, warranties or undertakings, whether oral or written, other than those set forth herein or referred to herein.

- C. **Amendments:** No alteration or variation of the terms of this Contract shall be valid unless made in writing and signed by the parties.
- D. **Taxes:** The fees shall be inclusive of all taxes imposed with respect to the provision of the Services hereunder, including any sales, use, excise, value-added, services, consumption, or other tax; provided, however, that County shall not be responsible for, and the fees shall not include, any taxes imposed on or arising from the following: (a) charges for goods and services provided by County to Riskconnect in connection with this Contract; (b) Riskconnect's income, revenue or property; or (c) any franchise or privilege taxes. All taxes applicable to the Services under this Contract shall be separately itemized on any invoice.
- E. **Delivery:** Time of delivery of Services is of the essence in this Contract. County reserves the right to refuse any Services and to cancel all or any part of the Services that do not conform to the Scope of Work in accordance with any cure periods and other terms set forth herein.
- F. **Acceptance of Services:** Unless otherwise agreed to in writing by County, acceptance of the Services or any portion thereof shall not be deemed complete unless in writing and until all the Services have actually been received, inspected, and tested to the satisfaction of County, including but not limited to the acceptance process requirements set forth in Article 5 (Acceptance Testing) and in Section 3.5 (Acceptance Process and Project Completion) of Attachment A-1 (Additional Scope of Services).
- G. **Warranty:** Riskconnect warrants that: (a) it has the right to grant the license to use the Software as set out in these Terms; (b) the Software will materially perform in conformity with its related documentation attached hereto; (c) the Software and the medium on which it is being provided to County is free from any virus at the time of delivery; and (d) support and services will be provided with reasonable skill and care conforming to generally accepted software industry standards.

Except as provided above, Riskconnect's licensors make no warranties of any kind, including but not limited to with respect to the service, and/or the Riskconnect application, whether express, implied, statutory or otherwise. Riskconnect's licensors make no representation, warranty, or guaranty as to the reliability, timeliness, quality, suitability, availability, accuracy or completeness of Riskconnect's application. Riskconnect's licensors do not represent or warrant that (a) the Riskconnect application will be available, secure, timely, uninterrupted or error-free, or any other application, software, hardware, system or data, (b) the Riskconnect system or the service will meet your requirements or expectations, (c) any data stored using the Riskconnect application will be accurate, reliable, or secure, (d) errors or defects in Riskconnect's application or the service will be corrected, or (e) the Riskconnect application or the systems used by Riskconnect to make the Riskconnect application available are free of viruses or other harmful components. To the maximum extent permitted by law, Riskconnect's licensors disclaim all conditions, representations and warranties, whether express, implied, statutory or otherwise, with respect to Riskconnect's application and the service, including, without limitation, any implied warranty of merchantability or fitness for a particular purpose. NOTHING IN THIS PARAGRAPH SHALL LIMIT RISKCONNECT'S WARRANTIES OR INDEMNIFICATION/DEFENSE OBLIGATIONS UNDER THIS CONTRACT, INCLUDING THOSE THAT RISKCONNECT MAKES AND/OR PROVIDES ON BEHALF OF RISKCONNECT'S LICENSORS.

The above warranties are in lieu of all other warranties express, implied, or statutory, including, but not limited to, the implied warranties of merchantability, quality, or fitness for a particular purpose.

- H. **Patent/Copyright Materials/Proprietary Infringement:** Unless otherwise expressly provided in this Contract, Riskconnect shall be solely responsible for clearing the right to use any patented or copyrighted materials in the performance of this Contract. Riskconnect warrants that any software as modified through Services provided hereunder shall not infringe upon or violate any patent, proprietary right, or trade secret right of any third party. Riskconnect agrees that, in accordance with the more specific requirement contained in Article Z below, it shall indemnify, defend and hold County and County Indemnitees harmless from any

and all such claims and be responsible for payment of all costs, damages, penalties and expenses related to or arising from such claim(s), including, but not limited to, attorney's fees, costs and expenses.

- I. **Assignment and Sub-Contracting:** The terms, covenants, and conditions contained herein shall apply to and bind the heirs, successors, executors, administrators and assigns of the Parties. Furthermore, neither the performance of this Contract nor any portion thereof may be assigned or sub-contracted by either Party without the express written consent of the other Party provided that either Party may assign this Contract without the other Party's consent to (i) a parent or subsidiary, (ii) an acquirer of assets, or (iii) a successor by merger. Any attempt by Riskconnect to assign or sub-contract the performance or any portion thereof of this Contract without the express written consent of County shall be invalid and shall constitute a breach of this Contract.
- J. **Non-Discrimination:** In the performance of this Contract, Riskconnect agrees that it shall comply with the requirements of Section 1735 of the California Labor Code and not engage nor permit any subcontractors to engage in discrimination in employment of persons because of the race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, marital status, or sex of such persons. Riskconnect acknowledges that a violation of this provision shall subject Riskconnect to all the penalties imposed for a violation of anti-discrimination law or regulation including but not limited to Section 1720 et seq. of the California Labor Code.
- K. **Termination:** Intentionally Omitted.
- L. **Consent to Breach Not Waiver:** No term or provision of this Contract shall be deemed waived and no breach excused, unless such waiver or consent shall be in writing and signed by the Party claimed to have waived or consented. Any consent by any Party to, or waiver of, a breach by the other, whether express or implied, shall not constitute consent to, waiver of, or excuse for any other different or subsequent breach.
- M. **Independent Contractor:** Riskconnect shall be considered an independent contractor, and neither Riskconnect, its employees nor anyone working under Riskconnect shall be considered an agent or an employee of County. Neither Riskconnect, its employees nor anyone working under Riskconnect, shall qualify for workers' compensation or other fringe benefits of any kind through County.
- N. **Performance Warranty:** Riskconnect shall perform all Services under this Contract, taking necessary steps and precautions to perform the Services in accordance with Article 1, Scope of Work. Riskconnect shall be responsible for the professional quality, technical assurance, timely completion and coordination of all documentation and other /services furnished by Riskconnect under this Contract. Riskconnect shall perform all Services diligently, carefully, and in a good and workman-like manner; shall furnish all labor, supervision, machinery, equipment, materials, and supplies necessary therefore; shall at its sole expense obtain and maintain all permits and licenses required by public authorities, including those of County required in its governmental capacity, in connection with performance of the Services; and, if permitted to subcontract, shall be fully responsible for all work performed by subcontractors.
- O. **Insurance:** Prior to the provision of services under this Contract, Riskconnect agrees to purchase all required insurance at Riskconnect's expense and to deposit with the County Certificates of Insurance, including all endorsements required herein, necessary to satisfy the County that the insurance provisions of this Contract have been complied with and to keep such insurance coverage and the certificates therefore on deposit with the County during the entire term of this Contract. In addition, all subcontractors performing work on behalf of Riskconnect pursuant to this Contract shall obtain insurance subject to the same terms and conditions as set forth herein for Riskconnect.

All self-insured retentions (SIRs) and deductibles shall be clearly stated on the Certificate of Insurance. If no SIRs or deductibles apply, indicate this on the Certificate of Insurance with a 0 by the appropriate line of coverage. Any SIR or deductible in an amount in excess of \$25,000 (\$5,000 for automobile liability), shall specifically be approved by the County Executive Office (CEO)/Office of Risk Management.

If Riskconnect fails to maintain insurance below for the full term of this Contract, the County may terminate this Contract in accordance with Article 9 ("Breach").

#### **Qualified Insurer**

The policy or policies of insurance must be issued by an insurer licensed to do business in the state of California (California Admitted Carrier) or have a minimum rating of A- (Secure A.M. Best's Rating) and VIII (Financial Size Category as determined by the most current edition of the **Best's Key Rating Guide/Property-Casualty/United States or ambest.com**).

If the insurance carrier is not a non-admitted carrier in the state of California and does not have an A.M. Best rating of A-/VIII, the County CEO/Office of Risk Management retains the right to approve or reject a carrier after a review of the company's performance and financial ratings.

The policy or policies of insurance maintained by Riskconnect shall provide the minimum limits and coverage as set forth below:

Coverage	Minimum Limits
Commercial General Liability	\$1,000,000 per occurrence \$2,000,000 aggregate
Automobile Liability including coverage for non-owned and hired vehicles	\$1,000,000 per occurrence
Workers Compensation	Statutory
Employers Liability Insurance	\$1,000,000 per occurrence
Technical, Media and Professional Liability Policy (Includes coverage for Software Engineers Errors and Omissions Liability)	\$10,000,000 per claim/in the aggregate

#### **Required Coverage Forms**

The Commercial General Liability coverage shall be written on Insurance Services Office (ISO) form CG 00 01, or a substitute form providing liability coverage at least as broad.

The Business Auto Liability coverage shall be written on ISO form CA 00 01, CA 00 05, CA 0012, CA 00 20, or a substitute form providing coverage at least as broad.

#### **Required Endorsements**

The Commercial General Liability policy shall contain the following endorsements, which shall accompany the Certificate of insurance:

- a. An Additional Insured endorsement using ISO form CG 2010 or CG 2033 or a form at least as broad naming the County of Orange, its elected and appointed officials, officers, employees, agents as Additional Insureds.
- b. A primary non-contributing endorsement evidencing that Riskconnect's insurance is primary and any insurance or self-insurance maintained by the County of Orange shall be excess and non-contributing.

All insurance policies required by this Contract shall waive all rights of subrogation against the County and members of the Board of Supervisors, its elected and appointed officials, officers, agents and employees when acting within the scope of their appointment or employment.

The Workers' Compensation policy shall contain a waiver of subrogation endorsement waiving all rights of subrogation against the County, and members of the Board of Supervisors, its elected and appointed officials, officers, agents and employees.

All insurance policies required by this Contract shall give the County 30 days' notice in the event of cancellation and 10 days for non-payment of premium. This shall be evidenced by policy provisions or an endorsement separate from the Certificate of Insurance.

If Contractor's Professional Liability, Technology Errors & Omissions and/or Network Security & Privacy Liability are "Claims-Made" policy(ies), Contractor shall agree to maintain coverage for two (2) years following the completion of the Contract.

The Commercial General Liability policy shall contain a severability of interest's clause also known as a "separation of insureds" clause (standard in the ISO CG 0001 policy).

Insurance certificates should be forwarded to the agency/department address listed in Article 31, Notices.

If Riskconnect fails to provide the insurance certificates and endorsements within ten days of notification by CEO/Purchasing or the agency/department purchasing division, County may terminate this Contract without penalty.

Riskconnect shall adjust the amounts of insurance coverage to whatever reasonable amount mutually agreed to by the Parties.

County shall notify Riskconnect in writing of mutually agreed upon changes in the insurance requirements. If Riskconnect does not deposit copies of acceptable certificates of insurance and endorsements with County incorporating such changes within thirty days of receipt of such notice, this Contract may be in breach without further notice to Riskconnect, and County shall be entitled to all legal remedies.

The procuring of such required policy or policies of insurance shall not be construed to limit Riskconnect's liability hereunder nor to fulfill the indemnification provisions and requirements of this Contract, nor act in any way to reduce the policy coverage and limits available from the insurer

Insurance certificates should be emailed to an individual employee of County designated by County.

Certificate holder must be as follows:

County of Orange  
c/o: CEO/County Procurement Office  
Attn: Insurance Desk  
1300 S. Grand Ave., Ste. A,  
2nd Floor Santa Ana, CA  
92705-4434

- P. **Changes:** Intentionally Omitted.
- Q. **Change of Ownership:** Riskconnect agrees that if there is a change or transfer in ownership of Riskconnect's business prior to completion of this Contract, the new owners shall be required under terms of sale or other transfer to assume Riskconnect's duties and obligations contained in this Contract and complete them to the satisfaction of County.
- R. **Force Majeure:** While not relieving Riskconnect of its duty to provide redundancy or establish backup and disaster recovery procedures as provided elsewhere in this Contract or its Attachments, no party to this Contract shall be liable for delay or failure in the performance of its contractual obligations arising from any one or more events which are beyond its reasonable control. Upon such delay or failure affecting one party, that party shall notify the other party and use all reasonable endeavors to cure or alleviate the cause of such delay or failure with a view to resuming performance of its contractual obligations as soon as practicable. Notwithstanding the foregoing, in every case the delay or failure to perform must be beyond the control and without the fault or negligence of the party claiming excusable delay. Performance times under this Contract or its Attachments shall be considered extended for a period of time equivalent to the time lost because of any delay which is excusable hereunder; provided, however, that, if any such delay shall, in the aggregate, last for a period of more than thirty (30) calendar days, or be expected to last for a period of more than thirty (30) calendar days, the party not relying on the excusable delay, at its option, may without penalty immediately terminate this Contract as it relates to the part of the Contract involved.
- S. **Confidentiality:** Riskconnect agrees to maintain the confidentiality of all County and County-related records and information pursuant to all statutory laws relating to privacy and confidentiality that currently exist or exist at any time during the Term of this Contract. All such records and information shall be considered confidential and kept confidential by Riskconnect and Riskconnect's staff, agents and employees.
- a) Riskconnect must restrict access to County Data to Riskconnect employees, affiliates' employees, or others who need to know that information to provide services to County or in the course of conducting Riskconnect's normal business operations. Riskconnect must maintain appropriate physical, electronic,



and procedural safeguards to protect County Data as governed in this Contract. Riskconnect shall protect personal data about County as a customer that may be collected at Riskconnect's website or at corporate events in accordance with Riskconnect's privacy statement found in Attachment E attached hereto and incorporated herein by reference. If County does provide Riskconnect with County Data, Riskconnect must only use it for the purposes described in this Contract, and Riskconnect must not sell, license, transmit or disclose this information outside of Riskconnect unless: (1) County expressly authorizes Riskconnect to do so; (2) it is necessary to allow Riskconnect's contracted service providers or agents to provide services for Riskconnect; (3) it is necessary to provide Riskconnect products or services to County; (4) it is necessary in connection with a sale of all or substantially all of the assets of Riskconnect or the merger of Riskconnect into another entity or any consolidation, share exchange, combination, reorganization, or like transaction in which Riskconnect is not the surviving entity; or (5) otherwise as Riskconnect is required by law. Notwithstanding the foregoing, Riskconnect is responsible for any disclosures of County Data by Riskconnect's service providers or agents made contrary to the terms of this Contract.

- b) As used herein, "Confidential Information" means all confidential and proprietary information of a Party disclosed to the other Party, whether orally, in writing or electronically, that is designated as confidential (except for County Data that need not be designated as confidential). Confidential Information (except for County Data) shall not include any information that: (i) is or becomes generally known to the public without breach of any obligation owed to the other Party; (ii) was known to a Party prior to its disclosure by the other Party without breach of any obligation owed to the other Party; (iii) was independently developed by a Party without breach of any obligation owed to the other Party; or (iv) is received from a third party without breach of any obligation owed to the other Party.
- c) Each Party agrees to protect the confidentiality of the Confidential Information of the other Party in the same manner that it protects the confidentiality of its own proprietary and confidential information of like kind (but in no event using less than reasonable care). If a Party is compelled by law to disclose Confidential Information of the other Party, it shall provide the other Party with prior notice of such compelled disclosure (to the extent legally permitted) and reasonable assistance, at the other Party's cost, if the other Party wishes to contest the disclosure. Riskconnect understands that County is subject to the requirements of the California Public Records Act. To the extent County receives a request for Riskconnect Confidential Information, County will provide written notice to Riskconnect of the request and give Riskconnect 30 days to obtain a court order limiting or restricting disclosure of the Confidential Information. In the event the order is not obtained, County will disclose the records to the extent required by the Public Records Act.
- d) If a Party discloses or uses (or threatens to disclose or use) any Confidential Information of the other Party in breach of confidentiality protections hereunder, the other Party shall have the right, in addition to any other remedies available to it, to seek injunctive relief to enjoin such acts, it being specifically acknowledged by the Parties that any other available remedies are inadequate.
- e) As a customer of the Riskconnect Service, County agrees that in the normal course of conversation, Riskconnect may disclose the fact that County is a customer.

T. **Compliance with Laws:** Riskconnect represents and warrants that Services to be provided under this Contract shall fully comply, at Riskconnect's expense, with all standards, laws, statutes, restrictions, ordinances, requirements, and regulations (collectively "laws"), including, but not limited to those issued by County in its governmental capacity and all other laws applicable to the Services at the time Services are provided to and accepted by County. Riskconnect acknowledges that County is relying on Riskconnect to ensure such compliance, and pursuant to the requirements of Article Z below, Riskconnect agrees that it shall defend, indemnify and hold County and County Indemnitees harmless from all liability, damages, costs and expenses arising from or related to a violation of such laws.

U. **Freight (F.O.B. Destination):** Intentionally Omitted.

- V. **Severability:** If any term, covenant, condition or provision of this Contract is held by a court of competent jurisdiction to be invalid, void or enforceable, the remainder of the provisions hereof shall remain in full force and effect and shall in no way be affected, impaired or invalidated thereby.
- W. **Attorney Fees:** In any action or proceeding to enforce or interpret any provision of this Contract, or where any provision hereof is validly asserted as a defense, each Party shall bear its own attorney's fees, costs and expenses.
- X. **Interpretation:** This Contract has been negotiated at arm's length and between persons sophisticated and knowledgeable in the matters dealt with in this Contract. In addition, each Party has been represented by experienced and knowledgeable independent legal counsel of their own choosing or has knowingly declined to seek such counsel despite being encouraged and given the opportunity to do so. Each Party further acknowledges that they have not been influenced to any extent whatsoever in executing this Contract by any other Party hereto or by any person representing them, or both. Accordingly, any rule of law (including California Civil Code Section 1654) or legal decision that would require interpretation of any ambiguities in this Contract against the Party that has drafted it is not applicable and is waived. The provisions of this Contract shall be interpreted in a reasonable manner to affect the purpose of the Parties and this Contract.
- Y. **Employee Eligibility Verification:** Riskconnect represents and warrants that it is and will be in full compliance with all Federal and State statutes and regulations regarding the employment of aliens (as that term is defined in applicable Federal statutes or regulations) and others and that all its employees performing work under this Contract meet the citizenship or alien status requirement set forth in Federal statutes and regulations. Riskconnect shall obtain, from all employees performing work hereunder, all verification and other documentation of employment eligibility status required by Federal or State statutes and regulations including, but not limited to, the Immigration Reform and Control Act of 1986, 8 U.S.C. §1324 et seq., as they currently exist and as they may be hereafter amended. Riskconnect shall retain all such documentation for all covered employees for the period prescribed by the law. Riskconnect shall indemnify, defend with counsel approved in writing by County, and hold harmless, the County, its agents, officers, and employees from employer sanctions and any other liability which may be assessed against Riskconnect or the County or both in connection with any alleged violation of any Federal or State statutes or regulations pertaining to the eligibility for employment of any persons performing work under this Contract.
- Z. **Indemnification:** Subject to the limitation set forth herein, Riskconnect shall indemnify, defend and hold the County and County-related entities (other local agencies governed by the County Board of Supervisors), agencies, departments, officers, employees, attorneys, agents, servants, franchises, successors and insurers harmless from and against any and all claims, costs, damages, losses, liabilities and expenses (including reasonable attorneys' fees and costs) arising out of or in connection with: (i) a claim arising from the breach by Riskconnect of this Contract; or (ii) a claim alleging Riskconnect's negligence or willful misconduct related to County Confidential Information, provided in any such case that the County (a) give written notice of the claim promptly to Riskconnect; (b) give Riskconnect sole control of the defense and settlement of the claim (provided that Riskconnect (1) shall provide to the County written confirmation that Riskconnect acknowledges Riskconnect's obligations to indemnify the County for such claim; (2) shall provide to the County evidence of Riskconnect's ability to defend and settle such claim, to the reasonable satisfaction of the County; and (3) may not settle any claim unless Riskconnect and the third party(ies) unconditionally release the County of all liability and such settlement does not affect the County's business or the Riskconnect Service); (c) provides to Riskconnect all available information and assistance at Riskconnect's sole cost and expense; and (d) has not compromised or settled such claim.

For clarity, Riskconnect shall not be liable for and shall not be required to hold harmless, provide defense or indemnification for the County's negligent or wrongful acts or omissions, or for errors and omissions caused by those persons or entities that the County utilizes to transmit claims' data to Riskconnect.

IN NO EVENT SHALL RISKCONNECT'S INDEMNIFICATION OBLIGATIONS RELATED TO CLAIMS OF THE TYPE COVERED BY RISKCONNECT'S GENERAL LIABILITY INSURANCE POLICY EXCEED \$3,000,000; PROVIDED, HOWEVER, THAT FOR CLAIMS OF THE TYPE THAT WOULD BE COVERED BY RISKCONNECT'S TECHNICAL, MEDIA AND PROFESSIONAL LIABILITY INSURANCE, THEN RISKCONNECT'S AGGREGATE INDEMNIFICATION LIABILITY SHALL BE LIMITED TO \$10,000,000.

AA. **Audits/Inspections:** At County's sole expense and upon not less than five (5) calendar days' notice, Riskconnect agrees to permit the County's Auditor-Controller or the County's authorized representative (including auditors from a private auditing firm hired by the County) access during normal working hours to all books, accounts, records, reports, files, financial records, supporting documentation, including payroll and accounts payable/receivable records, and other papers or property of Riskconnect for the purpose of auditing or inspecting any aspect of performance under this Contract. The inspection and/or audit shall be confined to those matters connected with the performance of the Contract including, but not limited to, the costs of administering the Contract. The County shall provide reasonable notice of such an audit or inspection. Failure to allow the County prompt and full access as stated above may result in a material breach of this Contract. The County reserves the right to audit and verify the Riskconnect's records before payment is made.

Riskconnect agrees to maintain such financial records for possible audit for a minimum of four years after final payment, unless a longer period of records retention is stipulated under this Contract or by law. Riskconnect agrees to allow interviews of any employees or others who might reasonably have information related to such records. Further, Riskconnect agrees to include a similar right to the County to audit records and interview staff of any subcontractor related to performance of this Contract.

BB. **Contingency of Funds:** This Contract is subject to and contingent upon applicable budgetary appropriations being made by the County of Orange Board of Supervisors for each County fiscal year (July 1 through June 30) during the term of this Contract. If such appropriations are not made, this Contract will be terminated without liability to County. Riskconnect acknowledges that funding or portions of funding for this Contract may also be contingent upon the receipt of funds from, and/or appropriation of funds by, the State of California to County. If such funding and/or appropriations are not forthcoming, or are otherwise limited, County may immediately terminate or modify this Contract without liability.

CC. **Expenditure Limit:** Intentionally Omitted.

**ADDITIONAL TERMS AND CONDITIONS:**

1. **Scope of Work:** This Scope of Work for this Contract is attached hereto as Attachments A, B, C, D, E, F, G, and H, all of which constitute part of this Contract. The services to be provided by Riskconnect thereunder are referred herein as the "Services."
2. **Term of Contract:** The Term ("Term") of this Contract shall be for five (5) years from December 10, 2021 through and including December 09, 2026 and may be renewed for a single additional two (2) year term upon the agreement of the Parties. The County does not have to give reason if it elects not to renew. Renewal periods may be subject to approval by the County of Orange Board of Supervisors. The County shall notify Riskconnect in writing with at least a sixty (60) day notice before the end of the Term.
3. **Calendar Days:** Any reference to the word "day" or "days" herein shall mean calendar day or calendar days, respectively, unless otherwise expressly provided.
4. **Compensation:** Riskconnect agrees to accept the specified compensation as set forth in Attachment B, Compensation/Cost, as full remuneration for performing all Services and furnishing all staffing and materials required, for any reasonably unforeseen difficulties which may arise or be encountered in the execution of the Services, for risks connected with the Services, and for performance by Riskconnect of all its duties and obligations hereunder.
5. **Acceptance Testing:** All deliverables shall be provided to the County by Riskconnect in conformity with all requirements, specifications, Acceptance Criteria, and time periods set forth or referenced in this Contract. Riskconnect shall at all times utilize complete and thorough Acceptance Testing Procedures, and appropriate Acceptance Criteria, all of which shall be subject to review and approval by the County's Program Manager, and no such activities shall be deemed completed until all Acceptance Criteria, whether set forth in this Contract or set forth in any schedule hereto or otherwise mutually agreed upon by the Parties in writing, have been successfully met.
  - a. **Acceptance Testing:** Following Riskconnect's notification to County that Riskconnect has completed any component or deliverable identified in this Contract, at a mutually agreed scheduled time thereafter,



County shall begin testing the component or deliverable to determine whether such component or deliverable conforms to the applicable specifications and/or standards (collectively, the "Acceptance Criteria"). After County has completed such testing or upon expiration of the agreed-upon testing period (the "Acceptance Testing Period"), County shall notify Riskconnect in writing either that: (a) the component or deliverable meets the Acceptance Criteria and that acceptance of such component or deliverable has occurred ("Acceptance"); or (b) the Acceptance Criteria have not been met and the reasons therefor. If the component or deliverable is identified as being part of a larger, integrated system being developed thereunder, then any Acceptance under the terms of this subsection shall be understood as being conditional acceptance ("Conditional Acceptance"), and such component or deliverable shall be subject to Final Acceptance, as described below.

- b. **Cure:** If County determines that a component or deliverable does not conform to the applicable Acceptance Criteria, County promptly shall deliver to Riskconnect a written exception report describing the nonconformity (the "Exception Report"). Within ten (10) calendar days following receipt of the Exception Report, Riskconnect shall: (a) perform a Root Cause Analysis to identify the cause of the nonconformity; (b) provide County with a written report detailing the cause of, and procedure for correcting, such nonconformity; (c) provide County with satisfactory evidence that such nonconformity will not recur; and (d) use best efforts to correct critical errors (as determined by County) and use commercially reasonable efforts to correct all other errors reasonably requested by County and accepted by Riskconnect; provided, however, that if the nonconformity of critical errors is incapable of cure within such ten (10) calendar day period then, within such ten (10) calendar day period, Riskconnect shall present to County a mutually agreeable plan to cure such nonconformity within a reasonable amount of time. Upon Riskconnect's notice to County that Riskconnect has cured any such nonconformity, County shall re-test the defective component or deliverable for an additional testing period of up to thirty (30) calendar days or such other period as the Parties may mutually agree upon in writing, at the end of which period the process described in subsection (b) above shall be repeated. In the event County rejects deliverable(s) a second time and Riskconnect disagrees with such rejection, then the Parties shall escalate the issue(s) to senior management of both parties for mutual resolution.
  - c. **Final Acceptance:** Upon achievement of Conditional Acceptance for all identified components or deliverables, County shall begin testing the system that is comprised of such components or deliverables using the applicable test procedures and standards to determine whether such system performs as an integrated whole in accordance with the Acceptance Criteria. After County has completed such testing or upon expiration of the testing period (the "Final Acceptance Testing Period"), County shall notify Riskconnect in writing that: (a) the system, and all components and deliverables that are a part thereof, meet the Acceptance Criteria and that final acceptance of the system and such components and deliverables has occurred ("Final Acceptance"); or (b) that the Acceptance Criteria have not been met and the reasons therefor. If County determines that the Acceptance Criteria have not been so met, the process described in subsection (b) above shall be initiated, with all references to "component or deliverable" being references to the "system," and all references to the "Acceptance Testing Period" being references to the "Final Acceptance Testing Period." Neither Conditional Acceptance, Acceptance nor Final Acceptance by County shall constitute a waiver by County of any right to assert claims based upon defects not discernible through conduct of the applicable test procedures and subsequently discovered in a component or deliverable or the system following County's Final Acceptance thereof. Nothing else, including County's use of the system, or any component thereof, shall constitute Final Acceptance, affect any rights and remedies that may be available to County and/or constitute or result in "acceptance" under general contract law, any state uniform commercial code or any other law
6. **Anti-Malware Protections:** Riskconnect's data center shall have strong access controls and secure practices, such as specialized authorization system(s), in effect at all times to prevent unauthorized physical and virtual access to hosted County systems. Riskconnect servers and network equipment hosted at the data center shall be properly secured from the threat of cyber hackers and viruses through appropriate intrusion detection tools, proactive 24x7x365 monitoring and prompt installation of new software updates, hot fixes and security patches.

Riskconnect shall use industry best practices regularly to identify, screen, and prevent any Disabling Device in resources utilized by Riskconnect in connection with the provision or receipt of the Services and shall not itself knowingly or intentionally install (and shall prevent its Subcontractors from knowingly and intentionally installing) any Disabling Device in resources utilized by Riskconnect, the County, or any Subcontractor, in connection with the provision or receipt of the Services. A “Disabling Device” is a virus, timer, clock, counter, time lock, time bomb, or other limiting design, instruction, or routine that would purposely and inappropriately erase data or programming or cause any resource to become inoperable or otherwise incapable of being used in the full manner for which such resource was intended to be used, and any device that may be used as a host to access County Data or launch attacks on County RCMIS Systems.

Riskconnect shall assist the County in reducing and mitigating the effects of any Disabling Device discovered in any resource related to the provision or receipt of the Services, especially if such Disabling Device is causing a loss of operating efficiency or data. Timers, clocks, counters, and time locks included as part of any commercial software, used by the County, by the manufacturer of that software shall not be considered Disabling Devices for purposes of this Article 6.

7. **Authority:** The Parties to this Contract represent and warrant that this Contract has been duly authorized and executed and constitutes the legally binding obligation of their respective organization or entity, enforceable in accordance with its terms.
8. **Authority Retained by County:** County shall have and at all times retain the exclusive right and authority to: (a) define, determine, and control the County’s RCMIS-related policies, strategies, objectives, and goals; (b) define, determine, and alter any or all of the County’s business processes; and (c) assess Riskconnect’s quality and performance. Riskconnect shall, at all times during the Term, perform and provide the Services in accordance with the strategies, processes, and policies described in the immediately preceding sentence, subject to the terms of this Contract.
9. **Breach:** The failure of Riskconnect to comply with any of the provisions, covenants or conditions of this Contract shall be a material breach of this Contract. In such event, the County may, and in addition to any other remedies available at law, in equity, or otherwise specified in this Contract:
  - a. Afford Riskconnect written notice of the breach and thirty (30) calendar days or such shorter time that may be specified in this Contract within which to cure the breach; and
  - b. Discontinue payment to Riskconnect for and during the period in which the Riskconnect is in breach; and
  - c. Offset against any monies billed by Riskconnect but yet unpaid by the County those monies disallowed pursuant to the above; and
  - d. Terminate this Contract immediately without penalty.
10. **Conditions Affecting Work:** Riskconnect shall be responsible for taking all steps reasonably necessary to ascertain the nature and location of the Services to be performed under this Contract and to reasonably know the general conditions which can affect the Services or the cost thereof. Any unreasonable failure by Riskconnect to do so shall not relieve Riskconnect from responsibility for successfully performing the Services without additional cost to the County. The County assumes no responsibility for any understanding or representations concerning the nature, location(s) or general conditions made by any of its officers or agents prior to the Effective Date of this Contract, unless such understanding or representations by the County are expressly stated in this Contract
11. **Conflict of Interest:** The County’s policies expressly prohibit it and its employees from engaging in activities involving a conflict of interest. Riskconnect shall not at any time during the Term of this Contract knowingly employ or otherwise engage any County employee for any purpose in any way related to Riskconnect’s performance of the Services hereunder. Riskconnect shall at all times exercise reasonable care and diligence to prevent any actions, circumstances, or conditions that could result in a conflict between Riskconnect (or any of its employees, agents, or subcontractors) and the best interests of the County. Such efforts by Riskconnect shall include establishing reasonable precautions to prevent its employees, agents, and subcontractors from making, receiving, providing, or offering to any employees of the County any gifts, entertainment, payments, loans, or other considerations that could appear to or be deemed to, or create

the impression of an attempt to, influence individuals to act in a manner contrary to the best interests of the County.

12. **County Data:**

- a) Subject to applicable law, the County shall permit Riskconnect and its subcontractors to have access to, and make appropriate use of, County Data (as defined below) solely to the extent Riskconnect and its subcontractors requires such access and use in order to properly and appropriately perform the Services as contemplated by this Contract. Riskconnect and its subcontractors may only access and use County Data in connection with performance of its duties under this Contract or as specifically directed by the County in writing and may not otherwise use, disclose, modify, merge with other data, commercially exploit, or make any other use of County Data or take, or refrain from taking, any other action that might, in any manner or form, adversely affect or jeopardize the integrity, security, or confidentiality of County Data, except as expressly permitted herein or as expressly directed by the County in writing. Riskconnect acknowledges and agrees that, as between the Parties, the County owns all right, title, and interest in, and all Intellectual Property Rights in and to, all County Data.
- b) **Ownership by the County:** All County Data, reports and other documents or materials created by the County through its use of the Riskconnect Service, including all Intellectual Property Rights in or pertaining to the same, shall be owned solely and exclusively by the County. The Parties further agree that all materials, documents, data or information obtained from the County or any County medium furnished to Riskconnect in the performance of this Contract shall at all times remain the property of the County. Such data or information may not be used or copied for direct or indirect use by Riskconnect after completion or termination of this Contract without the express written consent of the County. All materials, documents, data or information, including copies, must be returned to the County upon expiration of the Term or termination of this Contract.
- c) As the Parties agree that County shall always own the information or material that County submits to the Riskconnect Service pursuant to this Contract ("County Data"), County expressly agrees to have sole responsibility for the accuracy, quality, integrity, legality, reliability, appropriateness, and intellectual property ownership or right to use of all of County Data. Except for Riskconnect's material breach related to County Data, Riskconnect shall not be responsible or liable for the deletion, correction, destruction, damage, loss or failure to store any of County Data.
- d) County is responsible for all activity occurring under County's User accounts and shall abide by all applicable local, state, national and foreign laws, treaties and regulations in connection with County's use of the Riskconnect Service, including those related to data privacy, international communications and the transmission of technical or personal data.

13. **County's Relationship Manager:** County represents that the individual designated as the County's Relationship Manager is and shall ensure that any replacement holder of such position shall be, an experienced manager who is knowledgeable as to the County, its respective businesses, business practices, functions, and related activities, and its respective systems, requirements, and needs. The County's Relationship Manager shall at all times: (a) act as the primary liaison between the County and Riskconnect's Relationship Manager; and (b) have overall responsibility for directing and coordinating all of the County's activities hereunder; and (c) be vested with the necessary authority to fulfill all of the responsibilities of the County's Relationship Manager described in this paragraph.

14. **Data Load Requirements:**

- a) **Integration of Non-Riskconnect Service Applications:** In the event County acquires, licenses or otherwise obtains a Non-Riskconnect Service Application, any exchange of data between County and any third-party provider of a Non-Riskconnect Service Application is solely between County and such third-party. Riskconnect provides no warranties or support for Non-Riskconnect Service Applications.
- b) Per County's requirements, Riskconnect may receive County data that may be sent from third parties in order to perform data interface services. Unless otherwise specified, Riskconnect is responsible for the execution and verification of all implementation and ongoing data interfaces referenced in Article 1 (Scope of Work) of this Contract provided that:

- i. County shall be responsible for the delivery of electronic files in generally accepted, standard, readable formats.
  - ii. County shall be responsible for the delivery of a data dictionary for each data interface. Tables and fields must have consistently defined relationships (referential integrity). Tables must be received as merged (de-normalized) to provide a single flat file for each component (i.e., Claim, Claim Transactions, Location Hierarchy etc.).
  - iii. County shall be responsible for data transmissions to Riskconnect using an encrypted secure FTP or secure web service protocol.
  - iv. For each one-time Implementation Data Interface, County shall provide Riskconnect a test file and a go-live file. For Implementation interfaces that are also on-going interfaces, the implementation and on-going data files must be of the identical format.
  - v. The County will work with Riskconnect to resolve verification issues.
15. **Disaster Recovery Plan:** Riskconnect shall maintain a disaster recovery plan in effect throughout the term of the Contract. The disaster recovery plan shall be subject to County's review upon reasonable notice to Riskconnect. Riskconnect shall maintain reasonable safeguards against the destruction, loss, intrusion and unauthorized alteration of printed materials and data in its possession. At a minimum, Riskconnect shall perform (i) incremental daily back-ups, (ii) weekly full backups, and (iii) such additional back-ups and other measures Riskconnect may determine to be necessary to maintain such reasonable safeguards (collectively herein "Disaster Recovery Plan"). County's Program Manager may identify and notify Riskconnect in writing of other items that the County's Program Manager reasonably deems appropriate for inclusion in the Disaster Recovery Plan.
16. **Disputed Amounts:** County may withhold payment of fees or any other charges otherwise due to Riskconnect under this Contract to the extent that the County disputes such charges in good faith. In such case, the County shall provide to Riskconnect a reasonably detailed written explanation of the basis for the dispute and shall continue to make payments of undisputed amounts as otherwise provided in this Contract. If any disputed amounts are later determined to have been improperly withheld (i.e., properly charged by Riskconnect), then the County shall be obligated to pay the withheld amount in accordance with this Contract, until paid in full. If any paid amounts are later disputed by the County and determined to have been improperly paid (i.e., improperly charged by Riskconnect), then Riskconnect shall promptly pay the County, in cash, the improperly paid amount. The failure of the County to withhold payment shall not waive any other rights the County may have with respect to disputed amounts or overpayments. Except as otherwise provided herein, any dispute relating to amounts owed by a Party hereunder, shall be considered a disagreement.
17. **Disputes:** Parties shall deal in good faith and attempt to resolve potential disputes informally. If the dispute concerning a question of fact arising under the terms of this Contract is not disposed of in a reasonable period of time by Riskconnect's Project Manager and the County's Project Manager, such matter shall be brought to the attention of the County Purchasing Agent by way of the following process:
  - a. Riskconnect shall submit to the County Agency/Department Project Manager assigned buyer a written demand for a final decision regarding the disposition of any dispute between the parties arising under, related to, or involving this Contract, unless the County, on its own initiative, has already rendered such a final decision.
  - b. Riskconnect's written demand shall be fully supported by factual information, and, if such demand involves a cost adjustment to this Contract, Riskconnect shall include with the demand a written statement signed by a senior official indicating that the demand is made in good faith, that the supporting data are accurate and complete, and that the amount requested accurately reflects the Contract adjustment for which Riskconnect believes the County is liable.
  - c. Pending the final resolution of any dispute arising under, related to, or involving this Contract, Riskconnect agrees to diligently proceed with the performance of this Contract, including the delivery of goods and/or provision of Services. Riskconnect's failure to diligently proceed shall be considered a material breach of this Contract.



- d. Any final decision of the County shall be expressly identified as such, shall be in writing, and shall be signed by the County Purchasing Agent or his designee. If the County fails to render a decision within 90 days after receipt of Riskconnect's demand, it shall be deemed a final decision adverse to Riskconnect's contentions.
18. **Documentation/meetings:** Riskconnect shall develop relevant documents necessary to complete the services and requirements as set forth in this Contract. The County's Project Manager and Riskconnect's Project Manager shall meet [by telephone is acceptable] on reasonable notice to discuss Riskconnect's performance and progress under this Contract. If requested, Riskconnect's Project Manager and other project personnel shall attend all meetings. Riskconnect shall provide such information that is requested by the County for the purpose of monitoring progress under this Contract.
19. **Employee Qualification and Verification:** Subject to and in accordance with applicable law, Riskconnect, prior to assigning an individual as Riskconnect Personnel and at Riskconnect's sole expense, shall have appropriately verified the qualifications of such individual, and including verifying employment history, conducting reference checks, verifying non-employer technical certifications or education completed or degrees awarded, performing drug testing, conducting fingerprinting and a security background check that includes investigation and identification of all state or federal misdemeanor or felony convictions of such individual, and criminal charges pending against such individual, during the immediately preceding seven (7) years, and performing such other types of verification as reasonably requested by the County. Within thirty (30) days of the Effective Date and every twelve (12) months on the anniversary of the Effective Date thereafter, Riskconnect will certify in writing to the County that each and every employee of Riskconnect and any subcontractor working on County's account or having access to County Data meets all employee qualifications required in this Contract and under law. Failure to provide such certification constitutes a material breach of this Contract.
20. **Errors and Omissions:** All Professional Services performed by Riskconnect to implement County's configuration of the Riskconnect Service shall be materially complete and shall be carefully checked by the professional(s) identified by Riskconnect as Project Manager, prior to submission to the County. If the County discovers any errors or omissions prior to approving Riskconnect's reports, files and other written documents, the reports, files or documents shall be returned to Riskconnect for correction in accordance with Section 3.5. Acceptance Process and Project Completion in Attachment A-1.
21. **Gratuities:** Riskconnect warrants that no gratuities, in the form of entertainment, gifts or otherwise, were offered or given by Riskconnect or any agent or representative of Riskconnect to any officer or employee of the County with a view toward securing this Contract or securing favorable treatment with respect to any determinations concerning the performance of this Contract. For breach or violation of this warranty, the County shall have the right to terminate this Contract, either in whole or in part, and any loss or damage sustained by the County in procuring on the open market any goods or services which Riskconnect agreed to supply shall be borne and paid for by Riskconnect. The rights and remedies of the County provided in this Article are not exclusive and are in addition to any other rights and remedies provided by law or under this Contract.
22. **Headings:** The various headings and numbers herein, the grouping of provisions of this Contract into separate clauses and paragraphs, and the organization hereof are for the purpose of convenience only and shall not limit or otherwise affect the meaning hereof.
23. **License Grant and Restrictions:** Riskconnect hereby grants the County a non-exclusive, non-transferable, right to use the Riskconnect Service and the services of its licensors, solely for the County's own internal business purposes, subject to the terms and conditions of this Contract. All rights not expressly granted to the County are reserved by Riskconnect and its licensors. Notwithstanding any access the County may have to the services of Riskconnect's licensors via the Riskconnect application, Riskconnect is the sole provider of the Riskconnect application and the County is entering into a contractual relationship solely with Riskconnect. In the event that the Riskconnect ceases operations or otherwise ceases or fails to provide the Riskconnect application, Riskconnect's licensors have no obligation to provide the Riskconnect application or to refund the County any fees paid by the County to Riskconnect. In the event that Riskconnect ceases operations or fails to provide the Riskconnect Service, Riskconnect agrees to refund the County any unused portion of fees

paid less any fees actually incurred by Riskconnect. The County shall not (i) license, sublicense, sell, resell, rent, lease, transfer, assign, distribute, timeshare, provide on a service bureau basis or otherwise commercially exploit or make available to any third party the Riskconnect Service (or the services of Riskconnect's licensors) or the Content in any way; (ii) modify or make derivative works based upon the Riskconnect Service or the Content; (iii) create Internet "links" to the Riskconnect Service or "frame" or "mirror" any Content other than on the County's own intranets or otherwise for the County's own internal business purposes; or (iv) reverse engineer or access the Riskconnect Service in order to (a) build a competitive product or service, (b) build a product using similar ideas, features, functions or graphics of the Riskconnect Service, or (c) copy any ideas, features, functions or graphics of the Riskconnect Service. The County shall not (i) modify, copy or create derivative works based on the services of Riskconnect's licensors; (ii) frame or mirror any content forming part of the services of Riskconnect's licensors, other than on the County's own intranets or otherwise for the County's own internal business purposes; (iii) reverse engineer the services of Riskconnect's licensors; or (iv) access the services of Riskconnect's licensors in order to (A) build a competitive product or service, or (B) copy any ideas, features, functions or graphics of the services of Riskconnect's licensors. User licenses cannot be shared or used by more than one individual User but may be reassigned from time to time to new Users who are replacing former Users who have terminated employment or otherwise changed job status or function and no longer use the Riskconnect Service or new users who are filling in temporarily for an absent worker. The County system administrator will have the system rights to re-assign userids on an as needed basis. There is an expectation that the administrator will abide by the spirit of the Contract and will not use this capability to create a scenario where Userid sharing is allowed.

The County's license to use the Riskconnect Service does not include a license to use applications provided directly by Riskconnect's licensors.

The County may use the Riskconnect Service only for the County's internal business purposes and shall not: (i) send spam or otherwise duplicative or unsolicited messages in violation of applicable laws; (ii) send or store infringing, obscene, threatening, libelous, or otherwise unlawful or tortious material, including material that is harmful to children or violates third party privacy rights; (iii) send or store viruses, worms, time bombs, Trojan horses or other harmful or malicious code, files, scripts, agents or programs; (iv) interfere with or disrupt the integrity or performance of the Riskconnect Service or the data contained therein; or (v) attempt to gain unauthorized access to the Riskconnect Service or its related systems or networks.

The County is responsible for all activity occurring under the County's User accounts and shall abide by all applicable local, state, national and foreign laws, treaties and regulations in connection with the County's use of the Riskconnect Service, including those related to data privacy, international communications and the transmission of technical or personal data.

24. **Licensing Provisions (Additional) – Backup Requirements:** In addition to the requirements in Article 15, Riskconnect shall maintain near real-time replication between datacenters to store County's data. In doing so, Riskconnect shall make commercially reasonable efforts to ensure: (a) All County Data is backed up to tape at each data center on a rotating schedule of incremental and full backups; (b) any backup tapes are cloned over secure links to a secure tape archive; and (c) any backup tapes are not transported off site and are securely destroyed when retired. Any backups of County Data shall not be considered in calculating storage used by County.

25. **Limitation of Liability:**

- a. No Consequential Damages. IN NO EVENT SHALL EITHER PARTY BE LIABLE FOR LOST PROFITS, REVENUES OR FOR SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER FOR BREACH OF CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY, EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES; EXCEPTING, HOWEVER, ANY DAMAGES OR OTHER COST, EXPENSE OR LIABILITY ARISING FROM AN INDEMNIFICATION/DEFENSE OBLIGATION IN THIS CONTRACT SHALL NOT BE CONSIDERED CONSEQUENTIAL DAMAGES.
- b. Maximum Aggregate Liability. IN NO EVENT SHALL EITHER PARTY'S AGGREGATE LIABILITY ARISING OUT OF THIS CONTRACT EXCEED THE AMOUNTS ACTUALLY

PAID OR PAYABLE BY COUNTY UNDER THIS CONTRACT IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO SUCH CLAIM. NOTWITHSTANDING, RISKONNECT'S AGGREGATE LIABILITY UNDER THIS CONTRACT WILL BE (i) \$3,000,000 FOR CLAIMS OF THE TYPE THAT WOULD BE COVERED BY RISKONNECT'S GENERAL LIABILITY INSURANCE POLICY AS IN EFFECT ON THE EFFECTIVE DATE OF THIS CONTRACT AND (ii) \$10,000,000 FOR CLAIMS OF THE TYPE THAT WOULD BE COVERED BY RISKONNECT'S TECHNICAL, MEDIA AND PROFESSIONAL LIABILITY INSURANCE POLICY (WHICH PROVIDES COVERAGE FOR TECH E & O, IP AND CONFIDENTIAL INFORMATION OBLIGATIONS) AS IN EFFECT ON THE EFFECTIVE DATE OF THIS CONTRACT.

- c. **No Liability of Riskconnect's Licensors.** IN NO EVENT SHALL RISKONNECT'S LICENSORS HAVE ANY LIABILITY TO COUNTY OR ANY USER FOR ANY DAMAGES WHATSOEVER, INCLUDING BUT NOT LIMITED TO DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, OR DAMAGES BASED ON LOST PROFITS, HOWEVER CAUSED AND, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, WHETHER OR NOT COUNTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

**Independent Allocations of Risk.** EACH PROVISION OF THIS CONTRACT, INCLUDING ALL EXHIBITS, SUPPLEMENTAL MATERIALS, ADDENDA, AND ANY ASSOCIATED BUSINESS ASSOCIATE AGREEMENT, THAT PROVIDES FOR A LIMITATION OF LIABILITY, DISCLAIMER OF WARRANTIES, OR EXCLUSION OF DAMAGES IS TO ALLOCATE THE RISKS OF THIS CONTRACT BETWEEN THE PARTIES. THIS ALLOCATION IS REFLECTED IN THE PRICING OFFERED BY RISKONNECT TO COUNTY AND IS AN ESSENTIAL ELEMENT OF THE BASIS OF THE BARGAIN BETWEEN THE PARTIES. EACH OF THESE PROVISIONS IS SEVERABLE AND INDEPENDENT OF ALL OTHER PROVISIONS OF THIS CONTRACT. THE LIMITATIONS IN THIS ARTICLE 25 WILL APPLY.

26. **Location of Performance:** Except where Riskconnect obtains the County's Program Manager's prior written approval, Riskconnect shall perform all of the Services only from or at Locations within the geographic boundaries of the United States.
27. **Monitoring and Measuring Tools and Processes:** Riskconnect shall implement measurement and monitoring tools and produce the metrics and reports necessary to measure its performance against any of the Service Levels and shall deliver to County such reports. Upon request in connection with an audit, and at no additional charge to the County, Riskconnect shall provide the County or its designees with information and access to tools and procedures used to produce such metrics.
28. **Non-Exclusivity:** As long as Riskconnect's or its licensor's confidential information are not infringed, nothing herein shall prevent the County from providing for itself or obtaining from any third party, at any time during the Term or thereafter, the Services, or any type of products or services in any way analogous, similar, or comparable to the Services, as applicable, or any other products or services. Nor shall anything in this Contract be construed or interpreted as limiting the County's right or ability during the Term to increase or decrease its demand for Services hereunder.
29. **Non-Solicitation of Employees:** Except as otherwise expressly provided in this Contract, during the Term and for the first twelve (12) months thereafter, neither Party shall, without the prior written consent of the other Party, directly or indirectly solicit, entice, encourage, or otherwise recruit any employee of such other Party whose duties and responsibilities include performing services directly or indirectly connected with performance under this Contract to leave such other Party's employ in order to accept employment or other engagement with the soliciting Party, its affiliates, or any other Person. Notwithstanding the foregoing, the Parties acknowledge and agree that this Contract shall not prohibit solicitations by either Party through general advertising or other publications of general circulation. In no way is this Article intended, nor shall it be deemed, to restrict or limit any individual's right to seek employment, but rather this Article is intended to, and shall, prevent each Party from actively recruiting the employees of the other Party (except as

provided in this Contract), thereby depriving such other Party of vital resources, in the securing, development, training, and deployment of whom it has expended considerable time and resources.

30. **No Third-Party Beneficiaries:** This Contract is an agreement by and between the Parties, and neither: (a) confers any rights upon any of the employees, agents, or contractors of either Party, or upon any other person or entity not a Party hereto; or (b) precludes any actions or claims against, or rights of recovery from, any person or entity not a Party hereto.
31. **Notices:** Except as expressly otherwise stated herein, all notices, requests, consents, approvals, or other communications provided for, or given under, this Contract, shall be in writing, and shall be deemed to have been duly given to a Party if delivered personally, or transmitted by facsimile to such Party at its telecopier number set forth below (with the original sent by recognized overnight courier or first class mail to the Party at its address set forth below), or sent by first class mail or overnight courier to such Party at its address set forth below, or transmitted by e-mail to the Party at its e-mail address set forth below (with the original sent by recognized overnight courier or first class mail to the Party at its address below), or at such other telecopier number, address or e-mail address, as the case may be, as shall have been communicated in writing by such Party to the other Party in accordance with this Article. All notices shall be deemed given when received, in the case of personal delivery or delivery by mail or overnight courier, or when sent, in the case of transmission by facsimile with a confirmation, if confirmed by copy sent by overnight courier within one (1) day after sending the facsimile. The County and Riskconnect contact information contained below may be changed by written notice to the other Party.

Contractor: Riskconnect, Inc.  
Attn: Chief Financial Officer  
1701 Barrett Lakes Boulevard, Suite 500  
Kennesaw, GA 30144-4517

For County: County of Orange  
County Procurement Office  
Attn: Yarida Guzman, Deputy Purchasing Agent  
1300 S Grand Avenue  
Building A – 2<sup>nd</sup> Floor  
Santa Ana, CA 92705

32. **News/Information Release:** Contractor shall not issue any news releases or make any contact with the media in connection with either the award of this Contract or any subsequent amendment of, or effort under this Contract. Contractors must first obtain review and written approval of said news media contact from County through the County DPA. Any requests for interviews or information received by the media should be referred directly to County. Contractors are not authorized to serve as a media spokesperson for County projects without first obtaining permission from County.
33. **Personnel Requirements (Additional):** Riskconnect shall, at all times, make available appropriate and sufficient numbers and types of Riskconnect Personnel, in addition to Riskconnect's Relationship Manager, to timely perform Riskconnect's obligations hereunder, in accordance with this Contract and all Attachments hereto.
34. **Policies and Procedures:** Riskconnect, its subcontractors, Riskconnect Personnel, and all other agents and representatives of Riskconnect, will at all times comply with and abide by all policies and procedures of the County that are attached to this Contract in connection with Riskconnect's performance of the Services. Riskconnect shall cooperate with the County in ensuring Riskconnect's compliance with the policies and procedures described in this Contract, and any material violations or disregard of such policies or procedures shall constitute a breach of this Contract. Without limiting the foregoing, Riskconnect agrees to the following:
- a) **Security and Policies:** At all times during the Term, Riskconnect shall provide all Services, use all resources related thereto, and use, operate, support, and maintain the RCMIS Systems, in a secure manner and in accordance with the County's User Provisioning Policy Attachment G and Data Classification Policy Attachment H, as modified, supplemented, or replaced by the County from time



to time, in its sole discretion, by providing Riskconnect with a written copy of such revised requirements, policies, or procedures reasonably in advance of the date that they are to be implemented and effective (collectively, the "Security Policies"). In the event that any revision, modification, supplement or replacement of any of the Security Policies causes Riskconnect to incur additional expense or deploy additional resources or otherwise increase the effort required by it to fulfill its obligations under this Contract, and Riskconnect so notifies County of such fact in advance and receives County's approval to proceed, Riskconnect shall be entitled (subject to amendment of this Contract) to receive additional fees sufficient to compensate Riskconnect for such additional expense, additional resources or increased effort. Riskconnect shall at all times use industry best practices and methods with regard to the prevention, detection, and elimination, by all appropriate means, of fraud, abuse, and other inappropriate or unauthorized access to and use of RCMIS Systems and the networks involved with the provision or receipt of Services, including the implementation and deployment network management and maintenance applications and tools, the use of appropriate encryption technologies, and the other security-related Services described in this Contract. Riskconnect shall, and shall cause the Riskconnect Personnel and subcontractors to, fully comply with and abide by all such Security Policies at all times during the Term.

- b) **Information Access:** Riskconnect shall at all times use appropriate safeguard and security measures so as to ensure the confidentiality and security of all County Data. At all times during the Term, Riskconnect shall, and shall cause the Riskconnect Personnel and subcontractors, and the employees or agents of any of the foregoing, to, fully comply with all of the County's policies and procedures regarding data access and security, including those prohibiting or restricting remote access to the RCMIS Systems and County Data, as set forth in the Security Policies. Riskconnect shall, and shall cause the Riskconnect Personnel and subcontractors to, fully comply with and abide by all such Security Policies at all times during the Term. The County shall authorize, and Riskconnect shall issue, any necessary information-access mechanisms, including access IDs and passwords, and in no event shall Riskconnect permit any such mechanisms to be shared or used by other than the individual Riskconnect Person to whom issued. Riskconnect shall provide each Riskconnect Person with only such level of access as is required for such individual to perform his or her assigned tasks and functions. From time to time throughout the Term, upon request from the County but at least once each Contract Quarter, Riskconnect shall provide the County with an accurate, up-to-date list of those Riskconnect Personnel having access to the RCMIS Systems, or County Data, and the respective security level or clearance assigned to each such Riskconnect Person. All RCMIS Systems, and all data contained therein, including County Data, used or accessed by Riskconnect Personnel: (a) shall be used and accessed by such Riskconnect Personnel solely and exclusively in the performance of their assigned duties in connection with, and in furtherance of, the performance of Riskconnect's obligations hereunder; and (b) shall not be used or accessed except as expressly permitted hereunder, or commercially exploited in any manner whatsoever, by Riskconnect, the Riskconnect Personnel or any subcontractor, at any time. Riskconnect acknowledges and agrees that any failure to comply with the provisions of this Article shall constitute a breach of this Contract and entitle the County to deny or restrict the rights of such non-complying Riskconnect Personnel to access and use the RCMIS Systems and County Data, as the County in its sole discretion shall deem appropriate.
- c) **Enhanced Security Measures:** The County may, in its discretion, designate certain areas, facilities, or RCMIS Systems as ones that require a higher level of security and access control. The County shall notify Riskconnect in writing reasonably in advance of any such designation becoming effective. Any such notice shall set forth in reasonable detail the enhanced security or access-control procedures, measures, or requirements that Riskconnect shall be required to implement and enforce, as well as the date on which such procedures and measures shall take effect. Riskconnect shall, and shall cause the Riskconnect Personnel and subcontractors to, fully comply with and abide by all such enhanced security and access measures and procedures as of such date.
- d) **General Security Standards:** At all times during the Term, Riskconnect shall maintain a level of security with regard to the RCMIS Systems and County Data for which Riskconnect has agreed in this Contract to provide or manage physical security, that in all events is at least as secure as each of the following levels of security: (a) that are maintained by Riskconnect with regard to its own systems,

- data, and facilities of a similar nature and import; and (b) that are common and prevalent in the industry and in accordance with industry best practices.
- e) **Breach of Security:** Any material breach or violation by Riskconnect or its subcontractors, or the employees or agents of any of the foregoing, or of the Security Policies, shall be deemed a material breach of a material obligation of Riskconnect under this Contract, and any chronic or critical breach by Riskconnect or its subcontractors, or the employees or agents of any of the foregoing, or of the Security Policies shall be deemed an incurable and material breach of a material obligation of Riskconnect under this Contract.
  - f) **Security Audits:** Each Contract Year, County may perform or have performed security reviews and testing based on an RCMIS infrastructure review plan. Such testing shall include all pertinent County security standards as well as any customer agency requirements, such as federal tax requirements. Riskconnect shall inform County of any security audit or assessment performed that includes County hosted content, within sixty (60) days of such audit or assessment.
  - g) **Preparation for Successor to this Contract:** At any time or times during the Term, at the written request of the County, Riskconnect shall provide the County with any information that the County is entitled to receive under this Contract that the County desires to use in preparing a request for proposal to solicit responses, or responding to proposals, for the purpose of entering into an agreement that would constitute the successor to this Contract. Such requested information may include, among other things, current and projected transactional or other relevant volumes, resource utilization and performance statistics and trends, forms utilization, and such other information, statistics, and materials related to the provision of the Services or the use, operation, support, and maintenance of the RCMIS Systems as the County shall reasonably deem necessary or appropriate.
  - h) **All Necessary Cooperation and Actions:** Riskconnect shall take such additional actions and perform such additional tasks as are necessary, appropriate, or reasonably requested by the County, during the Term, to ensure a timely and seamless transition to a successor contractor.
35. **Project Manager – County and Riskconnect:** The County shall appoint a Project Manager to act as liaison between the County and Riskconnect during the Term of this Contract. Riskconnect shall appoint a Project Manager to direct Riskconnect's efforts in fulfilling Riskconnect's obligations under this Contract and who will ensure that Riskconnect personnel interface with County personnel in a manner conducive to facilitating Riskconnect's performance of the Services under this Contract, including the timely evaluation and testing of the Services. Riskconnect's Project Manager and personnel shall be subject to approval by County and shall not be changed without the written consent of the County's Project Manager. The County's Project Manager shall have the right to require the removal and replacement of Riskconnect's Project Manager and/or personnel from providing services to County under this Contract. The County's Project Manager shall notify Riskconnect in writing of such action. Riskconnect shall accomplish the removal within thirty (30) calendar days after written notice by the County's Project Manager. County is not required to provide written reason, rationale or factual information in the event it elects to request the removal of Riskconnect Project Manager from providing services to County under this Contract.
36. **Promotional/Advertisement:** County owns all rights to the name, trademarks, logos and symbols of County. The use and/or reproduction of County's name, trademark, logo and/or symbol for any purpose, including commercial advertisement, promotional purposes, announcements, displays or press releases, without County's express prior written consent is expressly prohibited. No use or reproduction may state or imply that County endorses Contractor's products or Services.
37. **Proprietary Rights (Ownership by Riskconnect):** Riskconnect alone (and its licensors, where applicable) shall own all right, title and interest, including all related Intellectual Property Rights, in and to the Riskconnect Service, the Content, the Computing Platform, the Software, and the Riskconnect Technology and any suggestions, ideas, enhancement requests, feedback, recommendations or other information provided by the County or any other party which results in mere configuration of the Riskconnect unless otherwise agreed in writing by the Parties (herein "Riskconnect IP"). This Contract does not convey to the County any rights of ownership in or related to the Riskconnect IP or the Intellectual Property Rights owned by Riskconnect's licensors, where applicable. The Riskconnect name, the Riskconnect logo, and the product

names associated with Riskconnect IP and its licensors are trademarks of Riskconnect or third parties, and no right or license is granted to use them unless prior written consent is granted by Riskconnect senior management. All Riskconnect IP, and all modifications or derivatives of such Riskconnect IP, including all Intellectual Property Rights in or pertaining to the same, shall be owned solely and exclusively by Riskconnect and its licensors.

38. **Publication:** No copies of sketches, schedules, written documents, computer-based data, photographs, maps or graphs, including graphic artwork, resulting from performance or prepared in connection with this Contract, are to be released by Riskconnect and/or anyone acting under the supervision of Riskconnect to any person, partnership, company, corporation, or agency, without prior written approval by the County, except as necessary for the performance of the Services of this Contract. All press releases, including graphic display information to be published in newspapers, magazines, etc., are to be administered only by the County unless otherwise agreed to by both Parties.
39. **Qualified Personnel:** In the event that Riskconnect fails to meet any of its obligations with respect to the required proficiency of any Riskconnect Personnel, Riskconnect shall promptly, as directed by the County, either: (a) take such action with respect to such Riskconnect Personnel, including promptly providing appropriate training, education, or orientation, as necessary for such Riskconnect Personnel to meet the applicable requirements set forth in this paragraph; or (b) in the event that the County has notified Riskconnect that such Riskconnect Personnel does not meet the applicable requirements, remove and replace such Riskconnect Personnel with an appropriately qualified individual, in accordance with this Contract, and such position shall be filled by a qualified person no later than thirty (30) days following the date of removal or replacement.
40. **Relationship Management:**
- a) **Status Reports:** Periodically during the Term of this Contract, but not less frequently than once each month, Riskconnect shall deliver to the Risk Manager a written report summarizing the progress of the Services and the operation of the RCMIS Systems during the preceding month, including problems that have occurred and could delay Riskconnect's performance of anticipated activities and expected problems during the upcoming month (each such report, a "Status Report"). At a minimum, each Status Report shall include: (a) the current status and progress of the performance of the Services and an assessment of how such status and progress compares to the Milestones, the Implementation Plan, and any other Attachments or deadlines set forth in the Scope of Work; (b) any actual delays; (c) any reasonably anticipated delays; (d) any failures, or correction of any failures; and (e) such other information as the County may reasonably request from time to time. Notwithstanding the foregoing, Riskconnect shall immediately notify (but in no event more than five (5) business days after Riskconnect first knew of such obstruction or delay) the County's Relationship Manager, in writing, in the event that Riskconnect is materially obstructed or delayed in its performance of the Services.
- b) **Status Meetings:** During the Term, representatives of the Parties shall meet and/or teleconference periodically as requested by the County to discuss matters arising under this Contract. Riskconnect costs in connection with the attendance and participation of such Party's representatives in such meetings, is addressed by Attachment B. The place and time, and whether to meet via teleconference or in person, shall be as determined as mutually agreed upon by the Parties.
41. **Remedies Not Exclusive:** The remedies for breach set forth in this Contract are cumulative as to one another and as to any other provided by law, rather than exclusive; and the expression of certain remedies in this Contract does not preclude resort by either Party to any other remedies provided by law.
42. **Riskconnect's Relationship Manager:** Riskconnect represents that the individual designated as Riskconnect's Relationship Manager is, and promises that any replacement holder of such position shall be, an experienced manager who is knowledgeable as to the County, its respective businesses, business practices, functions, and related activities, and its respective RCMIS Systems, requirements, and needs. The County shall have the right to interview, as the County deems necessary, and participate (by providing input and recommendations) in the final selection of, Riskconnect's Relationship Manager. Without the prior written consent of the County's Program Manager which consent shall not be unreasonably withheld,

Riskconnect shall not: (a) designate a replacement for Riskconnect's Relationship Manager; or (b) voluntarily replace or reassign the individual serving as Riskconnect's Relationship Manager during the first twelve (12) months after the date that such individual commences performing the duties of Riskconnect's Relationship Manager hereunder. Riskconnect's Relationship Manager shall at all times: (i) act as the primary liaison between Riskconnect and the County's Relationship Manager; (ii) have overall responsibility for directing all of Riskconnect's activities hereunder, directing the performance of all Services from inception through completion; (iii) be vested with the necessary authority to fulfill all of the responsibilities of Riskconnect's Relationship Manager described in this Contract; and (iv) coordinate and conduct periodic program review sessions with the County to discuss costs, Attachments, and any relevant technical aspects of Riskconnect's performance under this Contract.

43. **Root Cause Analysis, Predictive Analysis and Resolution:**

- a. **Process:** Upon Riskconnect's discovery of, or, if earlier, Riskconnect's receipt of a notice from the County in respect of,
- i. Riskconnect's failure to meet a SLR, or
  - ii. Riskconnect's failure to provide the Services, or to operate, support, and maintain the RCMIS Systems, in accordance with the SLRs and this Contract.

Riskconnect shall comply with the processes established in Attachment C concerning Riskconnect Service Levels. The correction of any such failure shall be performed entirely at Riskconnect's expense.

- b. **Pending Disputes:** Unless otherwise directed by the County, and notwithstanding the pendency of any disagreement or Root Cause Analysis as to the cause of a defect, malfunction, or difficulty, Riskconnect shall take prompt and reasonable steps to correct such defect, malfunction, or difficulty at its sole cost.
- c. **Compatibility of Resources:** Riskconnect shall ensure that the RCMIS Systems, all Services, and all software, assets, hardware, equipment, and other resources and materials (collectively, the "Riskconnect Resources") that are provided by Riskconnect to the County, otherwise utilized by Riskconnect, or approved by Riskconnect for utilization by the County, in connection with the use or operation of the RCMIS Systems, or with the providing or receiving of the Services, shall be successfully and fully integrated and interfaced, and shall be compatible, with, all applicable County software, services, systems, items, and other resources (collectively, the "County Resources") that are owned by or leased or licensed to the County, or that are provided to the County by third party service providers. To the extent that any interfaces need to be developed or modified in order for the Riskconnect Resources to integrate fully and successfully, and be compatible, with the County Resources, Riskconnect shall be responsible for the development or modification of such interfaces and for such integration, and all such activities shall be deemed to be Services within the scope of this Contract.

44. **Security Deliverables and Documents:** As this Contract may involve Riskconnect having direct access to County proprietary information, IT staff, and systems; the County has outlined various deliverables and documents in relation to Riskconnect Data Security that shall be provided by the Riskconnect to the County within thirty (30) days of Contract execution. The County shall review these deliverables and documents prior to final approval and actual access to the resources or transfer of any information related to this Contract.

Deliverables and Documents to be provided by Riskconnect as follows:

- a. Staff Related Items
- Pre-Employment Screening Policy/Procedure
  - Background Checking Procedure
  - Staff Roster and Duties
  - Non-US Staffing Duties
- b. Security Related Items
- IT. Security Staff Usage Policy
  - IT. Security Policies and Procedures
  - IT. Operations Security Policy



- Document & Intellectual Property Management Policies
- c. IT Systems Related Items
- Policies Related to Data, Tapes, and Resources that will be removed from County Facility
  - Policies Related to Access to County Data Internally or Via Remote Access
45. **Security Management Services:** Riskconnect shall provide appropriate and comprehensive security Services, that meet the County's security requirements, using industry best practices and methods, and commercially available technology, to at all times ensure the security and integrity of the RCMIS Systems and County Data, and to protect against unauthorized access to, use of, or intrusion into, the Systems and unauthorized disclosure of the County Data. Without limiting anything set forth in the Scope of Work, such Services shall include operating RCMIS Systems under a best practices-based security plan that conforms in all respects to the requirements of all applicable federal, state and local laws, regulations, and ordinances relating to security, privacy, or confidentiality, ensuring compliance with County and County security policies and procedures provided or made available to Riskconnect, performing all necessary and appropriate security-related audits and reports, and promptly providing County with a full and complete copy of each such report.
46. **Service Level Commitment:** Except as otherwise specified in this Contract, from and after the Effective Date, Riskconnect shall perform the Services at levels that are equal to or better than the Service Levels applicable to such Services. Riskconnect shall be responsible for meeting or exceeding the applicable Service Levels even where doing so is dependent on the provision of Services by subcontractors or other non-Riskconnect personnel. The Service Level methodology applicable to the Service Levels is set forth in Attachment C. Any resources utilized by Riskconnect pursuant to the terms hereof shall incorporate methods permitting measurement of all performance-related Service Levels. Riskconnect shall measure and compare the actual or observed performance resulting from Riskconnect's performance of the Services with the Service Levels during each month. Riskconnect shall prepare and deliver or make available to the County's Program Manager by the tenth (10th) business day of the following month, a Service Level report in a format to be agreed to by the County's Program Manager and Riskconnect.
47. **Set-Off:** County may set off against any and all amounts otherwise payable to Riskconnect pursuant to any of the provisions of this Contract: (i) any and all amounts claimed by the County in good faith to be owed by Riskconnect to the County pursuant to any of the provisions of this Contract; and (ii) any and all amounts claimed by the County in good faith to be owed by Riskconnect pursuant to any other written agreement between the Parties. Within twenty (20) days after any such set-off by the County, the County shall provide Riskconnect with a written accounting of such set-off and a written statement of the reasons therefore.
48. **Stop Work:** In the event that the County's Program Manager determines, at any time during the Term of this Contract that the quality or continuity of any portion of the Services have been materially and adversely affected in any way, or that any such material and adverse effect seems reasonably likely to occur, then upon notice the County's Program Manager may direct Riskconnect to stop and proceed no further until such time as Riskconnect shall have: (i) analyzed the cause of such condition; (ii) developed a reasonable plan for resuming such Services in such a manner as to eliminate or avoid such condition. Riskconnect shall not re-commence the performance of any Services until County's Program Manager has issued an approval in writing. The issuance of a stop order shall not constitute, nor shall be construed as, a breach of this Contract by County.
49. **Termination by Riskconnect:** Riskconnect may terminate this Contract solely if: (a) the County has not made payments due and payable hereunder, (b) the aggregate total of such non-payments exceeds Fifty Thousand Dollars (\$50,000), (c) such non-payments are not subject to a good faith dispute, (d) Riskconnect provides County with a minimum of thirty (30) days written notice after the non-payment's due date of its intent to terminate; and (v) no less than sixty (60) additional calendar days pass with such payment not having been made.
50. **Termination-County Right:** Notwithstanding anything to the contrary herein, the County has the right to terminate: (a) the Term of this Contract with regard to the Services, or (b) any portion the Services (e.g., a Service area or subcomponent), then being provided by Riskconnect by delivery of a Termination Notice to Riskconnect, if Riskconnect commits a material breach under this Contract and provides notice of said breach

and an opportunity to cure as required by the Contract. Any such termination shall not constitute the County's exclusive remedy for such breach, nor shall such a termination cause the County be deemed to have waived any of its rights accruing hereunder prior to such breach. If the County terminates the Term or any portion of the Services as a result of a claimed breach by Riskconnect pursuant to the terms of this Article, and Riskconnect does not agree that a breach was committed, then Riskconnect shall have the right to avail itself of all remedies available to it at law or in equity. In the event that it is subsequently and finally determined by a court of competent jurisdiction, or otherwise mutually agreed by the Parties in writing, that the circumstances claimed by the County to constitute a breach by Riskconnect, and that formed the basis of a termination of the Term of this Contract or any portion of the Services by the County pursuant to this Article, did not in fact constitute a breach, then the Term of this Contract, or applicable portion of the Services, shall be deemed to have been mutually terminated by the Parties, as of the Termination Date specified by the County in the Termination Notice originally delivered with respect to such termination shall thereafter in all respects govern such termination

51. **Termination - Orderly:** Upon ending of the Term, termination or other expiration of this Contract, each Party shall promptly return to the other Party all papers, materials, and other properties of the other held by each for purposes of performance of this Contract. In addition, each Party shall assist the other Party in orderly termination of this Contract and the transfer of all aspects, tangible and intangible, as may be necessary for the orderly, non-disruptive business continuation of each Party. Upon expiration of the Term or termination of this Contract, Riskconnect will return all County Data to the County in CSV file format within thirty (30) days of the expiration of the Term of termination date.

52. **Definitions:**

- A. Software. The term "Software" means the proprietary computer software programs of Riskconnect and its third party software licensors and all related materials, improvements, updates, licensed internal code, embedded third party software, new releases, fixes, enhancements, derivative products and information utilized by Riskconnect in providing County access to the Riskconnect Service and other services under this Contract.
- B. Service or Services. The terms "Service" and "Services" have the meaning set forth in Paragraph 1, Scope of Work.
- C. Update. The term "Update" means any bugs, patches, fixes, enhancements, improvements to the Software and any addition of new features pertaining only to County's existing modules.
- D. Upgrade. The term "Upgrade" means platform changes, addition of new modules or new integration points or the creation of new versions.
- E. Users. The term "User(s)" means County employees, representatives, consultants, contractors, agents or third parties who are authorized to use the Riskconnect Service on County's behalf and have been supplied user identifications and passwords by County or by Riskconnect at County's request subject to the requirements of Attachment G.
- F. RCMIS. The term "RCMIS" means Risk and Claims Management Information System, otherwise referred herein as the Riskconnect Service.
- G. Riskconnect Technology. The term "Riskconnect Technology" means all of Riskconnect's and its licensors' proprietary technology (including software, hardware, products, processes, algorithms, user interfaces, know-how, techniques, designs and other tangible or intangible technical material or information) made available to County by Riskconnect in providing the Riskconnect Service.
- H. Riskconnect Service. The term "Riskconnect Service" means County's customized version of Riskconnect's web-based RCMIS Software described in and implemented pursuant to Contract MA-017-14011355 (prior agreement between the Parties dated December 10, 2013), any Subscription Orders issued under MA-017-14011355 and any Statements of Work and/or Subscription Orders issued under this Contract, to which County is being granted access under this Contract.
- I. Incident. The term "Incident" means any event which is not part of the standard operation of a Service and which causes, or may cause, an interruption to, or a reduction in, the quality of that Service.

- J. Maintenance Window. The term “Maintenance Window” means a County-approved period of time during which preventive maintenance that could cause disruption of service may be performed.
- K. Malware. The term “Malware” means software designed to infiltrate or damage a computer system without the owner’s informed consent. Software is considered Malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, trojan horses, most rootkits, spyware, dishonest adware, crimeware and other malicious and unwanted software.
- L. Resolve or Resolution. The terms “Resolve” and “Resolution” mean to repair, replace, reconfigure, reinstall, re-route, or otherwise provide a complete solution to an Incident that returns the System and/or End User(s) to non-degraded full functionality.

**- SIGNATURE PAGE TO FOLLOW -**

### CONTRACT SIGNATURE PAGE

IN WITNESS WHEREOF, the Parties hereto have executed this Contract on the dates shown opposite their respective signatures below.

#### RISKONNECT, INC.\*

James Wetekamp President

---

Print Name Title

DocuSigned by:  
*James Wetekamp* 11/10/2021  
D832EBA7535B4C5... Date

Teri McEvily, CFO CFO

---

Print Name Title

DocuSigned by:  
*Teri McEvily, CFO* 11/10/2021  
0FC5E71C8D7545D... Date

\*\*\*\*\*

#### COUNTY OF ORANGE, A political subdivision of the State of California

Print Name Title

---

Signature Date

---

\*\*\*\*\*

#### APPROVED AS TO FORM, Office of the County Counsel, County of Orange, California

Brittany McLean Deputy County Counsel

---

Print Name Title

DocuSigned by:  
*Brittany McLean* 11/10/2021  
9713A4081D4343D... Date



**ATTACHMENT A**  
**SCOPE OF SERVICES - SUBSCRIPTION ORDER**

Contractor shall provide County the following SaaS licenses and subscriptions to access and use the Web-based version of Contractor's Riskconnect Service. The Riskconnect Service referenced is the customized version described in and implemented pursuant to Contract MA-017-14011355 (prior agreement between the Parties dated December 10, 2013), any Subscription Orders issued under MA-017-14011355 and any Statements of Work and/or Subscription Orders issued under this Contract.

All licenses, subscriptions and support provided by Contractor under this Contract shall be consistent with the Riskconnect Service already implemented and in operation in County (including all functionality) and this Contract shall not be construed to limit or reduce the scope thereof. Except as otherwise set forth in this Attachment A, County's right to access and use the Riskconnect Service are governed by the terms and conditions of this Contract.

User Licenses	Description	Quantity
Business Insights Advanced		1
Operations User with Reports (Existing Clients Only)		4
Operations User (Existing Clients Only)		7
eComposer License		10
Administrator User		1
Full User		7

Data Infrastructure & Storage Subscriptions	Description	Quantity
File Storage (GB)		50
Riskconnect Infrastructure		2

Data Subscription	Description
Ongoing Data- Monthly	ISO CMS – Bi-Directional
Ongoing Data- Daily y	ISO Query – Bi-Directional
Ongoing Data- Daily	CAPS+ Inbound

Customer Success Services	Description	Quantity
Annual Customer Support Hours		34

**Annual Data Services Support:** County agrees to Contractor's Data Transfer Protocols as outlined here: <https://riskconnect.com/legal-dtps/>

## ATTACHMENT A - 1 ADDITIONAL SCOPE OF SERVICES

Capitalized terms used but not defined in this Attachment A-1 shall have the meanings accorded to them in the Contract. This SOW is governed by the terms and conditions of the Contract. In the event of a conflict between the Contract and the terms of this Attachment A-1, the Contract shall prevail.

### SOW

This SOW sets forth the requirements for adding a semi-monthly Sedgwick Juris (E02) inbound data load. It also covers configuration of WC related fields, addition of Task types and configuration of an additional workflow notification.

1. **Deliverables.** The deliverables to be performed by Riskconnect under this SOW are expressly limited to:
  - 1.1. **Configuration of the Riskconnect Service**
    - 1.1.1. Configure up to 20 custom fields to be placed in a new Section on the existing WC Claim Record Type and Page Layout.
    - 1.1.2. Configure a workflow notification with reminder to review case 60 days after reserve set.
    - 1.1.3. Configure 10 record types for Tasks with up to 10 fields per record type and page layout.
2. **Riskconnect Service Data Deliverables.** Data shall be provided pursuant to the data transfer protocols (“DTPs”) as outlined here: <https://riskconnect.com/legal-dtps/>. Untimely or incomplete receipt of County Data, poor data quality, or failure to provide data in a consistent layout and format will impact project. County agrees to ensure all completed data sets described in this section are provided either from County or its third-party Service Providers to Riskconnect pursuant to the Project Plan.

Riskconnect Service: Data Deliverables				
Data Deliverables: Ongoing Data Interfaces	Interface Type (Standard/ Custom)	Initial Data	Ongoing Data	Frequency
Sedgwick Juris (E02) Inbound	Standard	Claim Summary Claim Transactions	Claim Summary Claim Transactions	Semi Monthly
<p><i>For ongoing data interfaces after go live, support needs resulting from issues outside of Riskconnect’s control (e.g.: data provider mistake resulting in interface failure, a load failure caused by lack of data arrival, etc.) will be provided using County’s Annual Customer Support Hours, provided that County has enough hours available as listed in Section 2.3 of Attachment B. In the event County does not have enough Annual Customer Support Hours available, Riskconnect shall provide a reasonable estimate on the support hours needed to address County’s support need. Upon County’s written approval of the reasonable estimate, Riskconnect must provide the professional support services and then bill County for the hours needed to address County’s support need at the rate listed in Section 5.5 and County agrees to pay for such service hours in accordance with the Contract to the extent the amount does not exceed the Contract’s not to exceed amount. Any such additional services may require an amendment to this Contract.</i></p>				
<p><i>*Standard Data Interfaces: County acknowledges receipt of the Riskconnect Sedgwick Juris Load Interface-4 specifications (“Product Overview”), provided to County on May 12, 2021 via secure content email (see Section 3.7 in this Attachment A-1 for a portion of the applicable specifications contained in the May 12, 2021 email for ease of reference). Riskconnect shall implement County’s standard interface in strict accordance with these written specifications as a bare minimum. In the event County wishes to further configure County’s standard interface beyond the specifications detailed in the referenced Product Overview, the additional configuration effort is noted in a separate line item above. County requested changes/modifications not explicitly outlined in above line item(s) will be addressed through the Project Change Order process and may require an amendment to the Contract.</i></p>				

3. **Project Implementation Methodology.**
  - 3.1. **Project Plan.**

The Riskconnect Project Manager will develop a written Project Plan to be mutually agreed upon by the Riskconnect Project Manager, Riskconnect Implementation Team and County’s Project Manager.
  - 3.2. **Project Management.**

- 3.2.1. **Project Stages.** Each implementation project progresses through four stages: Plan, Build, Deploy, and Close. Each stage utilizes various processes and techniques to properly plan, document, execute, and test project work.
- 3.2.2. **Project Scheduling and Status Reporting.** Riskconnect will build, with input from County, the project schedule which will detail the initial, high-level schedule of project stages and major milestones throughout the plan stage. As the project moves into the build stage, the schedule will be approved and finalized by both County and Riskconnect. Riskconnect will provide County with regular project status updates. These status updates consist of recurring status calls on a schedule mutually agreed upon between County and Riskconnect and the following supporting project status documentation.
  - 3.2.2.1. Current Project Status Report with project health summary, deliverable status, issues list, and action items tracking.
  - 3.2.2.2. Current project schedule.
  - 3.2.2.3. Requirements documentation including user stories and acceptance criteria.
  - 3.2.2.4. Project Hours Burn report with justification for the hours used.
  - 3.2.2.5. Change request documentation.
- 3.2.3. **Change Control Process.** When County identifies a need for a change to this Attachment A-1 and submits a Project Change Order (PCO) request to Riskconnect Project Manager, Riskconnect may complete an analysis of the potential impact to time and cost resulting from the PCO request or deny the PCO request. Riskconnect's analysis will define the estimate and costs Riskconnect would charge to implement the PCO request.
  - 3.2.3.1. **PCO Impact Analysis.** If Riskconnect does not deny the PCO request, Riskconnect will perform a detailed analysis of the PCO request, analyzing both the effort to complete the work and the impact to the Project Plan. Riskconnect then will provide the estimate and costs, and impacts to project schedule, to County for review. An estimate may be required to understand the cost impact even if the PCO is not implemented.
  - 3.2.3.2. **PCO Implementation Process.** If County approves in writing the change based on the analysis provided by Riskconnect, the Riskconnect Project Manager shall assign resources to proceed with the change, taking into account its priority with current project activities. The Riskconnect Project Manager will add a new task or tasks (including effort, duration, and resources) to the Project Plan under a task designated for PCO changes. Depending on the degree of change in scope of work, the Parties may need to execute an amendment to this Contract.
  - 3.2.3.3. **Monitoring.** Progress of the PCO effort is monitored on a regular basis until the change is completed. When the change is completed and approved by County, the PCO request is closed.
- 3.2.4. **Project Risks and Mitigation.**
  - 3.2.4.1. **Risk Management Process.** The risk management process identifies, quantifies, and mitigates risks to the project. This is a process that needs to be continually reviewed by Riskconnect with County during implementation.
  - 3.2.4.2. **Risk Identification and Tracking.** The Riskconnect Project Manager will meet regularly with County's Project Manager to identify, quantify, and prioritize risks, and to review the status of previously identified risks. Other team members representing various focuses of the project, such as business analysts, technical analysts, or project managers may be involved, but only to the extent necessary. The risk identification and tracking process will be performed by Riskconnect iteratively through implementation.

- 3.2.4.3. **Risk Status Reporting.** The Riskconnect Project Manager will report on the status of the identified risks in the project status reports.
- 3.2.5. **Project Team.** Riskconnect and County will provide resources to ensure timely completion of implementation tasks specified in this Attachment A-1. Riskconnect shall accept the fees listed on Attachment B as full compensation for Riskconnect project team members who work on the project and interact across the project team. Commonly required project roles are summarized below.
  - 3.2.5.1. **County Executive Stakeholder.** The County Executive Stakeholder shall serve as an escalation point for the County should there be a dispute related to the project and/or the budget.
  - 3.2.5.2. **County Project Manager.** The County Project Manager for the Attachment A-1-Additional Scope of Services is responsible for the following:
    - 3.2.5.2.1. Serve as the primary point of contact with Riskconnect and support and facilitate decision making during the performance of implementation services and after Go-Live of the services.
    - 3.2.5.2.2. Monitor the progress of services associated with the implementation services.
    - 3.2.5.2.3. Help Riskconnect schedule meetings, attend meetings and ensure that the relevant County team members are present, unless other arrangements are made by County.
    - 3.2.5.2.4. Manage and oversee communication and acceptance of deliverables with Riskconnect via Acceptance Testing.
    - 3.2.5.2.5. Ensure that project deliverables, agreed upon by County and Riskconnect, are provided to Riskconnect in a timely and agreed upon format.
    - 3.2.5.2.6. Provide information for setup of Riskconnect required to ensure project completion in accordance with the Project Plan.
  - 3.2.5.3. **County Resources (Technical).** They will:
    - 3.2.5.3.1. Support data mapping and provide consultation for any data interfaces.
    - 3.2.5.3.2. Ensure reasonable access to Riskconnect from County's network for all County systems reasonably needed.
    - 3.2.5.3.3. Configure County's chosen Identity Management System to pass credentials to the Riskconnect system.
  - 3.2.5.4. **Riskconnect Project Manager.** The Riskconnect Project Manager is Riskconnect's primary contact for County. The Riskconnect Project Manager is responsible for managing the Project Plan, budget, scope, PCO, risk management and resource alignment and facilitating project meetings and other critical activities throughout the project duration. They also oversee resolution of any issues relating to the project and report issue status to the County Project Manager.
  - 3.2.5.5. **Riskconnect Delivery Manager.** The Riskconnect Delivery Manager is Riskconnect's second point of contact for County and project escalation point. The Riskconnect Delivery Manager is responsible for resource availability, resource management, project progress and quality oversight.
  - 3.2.5.6. **Riskconnect Project Resources.** These Riskconnect team members provide solution design and configuration, business requirements documentation, technical



and solutions consulting and UAT support, including all services that must be performed to provide all deliverables in accordance with this Contract.

### 3.3. **Project Assumptions.**

Riskconnect shall have primary responsibility for project methodology and implementation, and the Project Plan.

#### 3.3.1. **Project Meetings and Activities.** The parties shall use commercially reasonable efforts to attend all scheduled project meetings and ensure active participation in and completion of project activities.

3.3.1.1. Cancellations of project meetings and delays in completing project activities may result in project delays and additional costs.

3.3.1.1.1. Repeated delays by County will be escalated to County and, if continued, will result in Riskconnect's decision to reassign project resources.

3.3.1.1.2. Repeated delays by Riskconnect shall be escalated to appropriate executive stakeholders and if not resolved after escalation shall be deemed a material breach and may result in County terminating this Attachment A-1 in accordance with the terms of the Contract provided that County shall reimburse Riskconnect for all reasonable and undisputed fees and expenses incurred prior to termination that are due under this Contract.

3.3.1.1.3. County may request project restart, and based on resource availability, Riskconnect will use commercially reasonable efforts to reschedule the project as promptly as possible. Additional costs required to restart project will be billed to County.

3.3.1.2. Any changes performed by County in the production environment are the responsibility of County. Any request for Riskconnect to review or remediate said changes may result in a Project Change Order.

3.3.1.3. All work completed by Riskconnect is charged to the project, including:

3.3.1.3.1. Attending meetings

3.3.1.3.2. Planning and scheduling activities

3.3.1.3.3. Preparing and responding to emails

3.3.1.3.4. Preparing and updating the Project Plan

3.3.1.4. Any additional "approved" services added to Attachment A-1 Additional Scope of Services, may be billed to County as Professional Support Services pursuant to Attachment B.

#### 3.3.2. **Global Services.**

3.3.2.1. Currency. All claim financial values will only be recorded in U.S. dollars. Currency conversion is not included in the scope of this SOW.

3.3.2.2. Language. The portal and platform will be deployed in English only.

#### 3.3.3. **Data Services.**

3.3.3.1. Any data services shall be completed in accordance with Riskconnect's Data Transfer Protocols.

3.3.3.2. County will provide reasonable timely access to County Data, County's resources and all required documentation (such as a data dictionary, control totals, codes, and code descriptions).

- 3.3.3.3. Data loading assumes that the data provided is in correct and usable format. If the data is not in a usable format, it will be returned to County to be cleansed.
- 3.3.3.4. For Claim Data loads, Riskconnect will map all cause, nature, and part codes to Riskconnect standard values.

#### 3.4. **Riskconnect Assumptions**

- 3.4.1. County will have reviewed and agreed to the Salesforce usage limits in this Contract.
- 3.4.2. County will access the solution via an internet connection using a modern browser, in line with the Salesforce platform's guidance maintained here:  
[https://help.salesforce.com/articleView?id=getstart\\_browser\\_overview.htm&type=5](https://help.salesforce.com/articleView?id=getstart_browser_overview.htm&type=5)
- 3.4.3. Users assigned to the System Administrator profile, or derivatives thereof, will have access to all data.
- 3.4.4. Riskconnect shall only be deployed in the Riskconnect Cloud (a SaaS model).

#### 3.5. **Acceptance Process and Project Completion**

- 3.5.1. **User Acceptance Tests and Testing.** Acceptance Tests will define the actions required to validate that the mutually agreed and project accepted design deliverables have been correctly tested. When executed, the Acceptance Tests carry out the solution detailed in the design deliverables and validate the requirements agreed upon during the project. Acceptance of a deliverable or set of deliverables signifies approval by Customer for functionality to be deployed to a production environment based on timing agreed in the Project Plan. The execution and completion of the Acceptance Tests and the performance of Acceptance Testing shall constitute and be referred to as "User Acceptance Testing" or "UAT" for purposes of this SOW.
  - 3.5.1.1. Customer is responsible for creating the test cases using its data and business requirements and executing UAT plan, including any interactions and dependencies with third parties.
  - 3.5.1.2. Customer and Riskconnect will mutually agree that the test cases are an accurate reflection of the design deliverables.
  - 3.5.1.3. Test cases that identify additional requirements outside of the agreed design deliverables are considered out of scope. Out of scope functionality and/or test cases, if required by the customer, may be submitted to Riskconnect through the PCO process.
  - 3.5.1.4. The Acceptance Test plan will align with the schedule and scope detailed in this SOW and any related PCOs.
  - 3.5.1.5. Riskconnect may provide Customer with sample test cases to facilitate the process.
- 3.5.2. **Acceptance Process and Deliverable Signoff.** Customer shall have ten (10) business days (or such period as identified in the Project Plan) after Riskconnect provides a deliverable to review and test such deliverable (the "Testing Period") in accordance with any Acceptance Tests specified during UAT.
  - 3.5.2.1. Customer's acceptance occurs upon its written notification of acceptance to Riskconnect. Customer shall not unreasonably withhold or delay its acceptance.
  - 3.5.2.2. Customer's failure to provide acceptance or rejection within the ten (10) business day period (or such period as specified in the Project Plan) will be deemed acceptance of the deliverable.
  - 3.5.2.3. In the event the deliverables, or any portion, do not satisfy any such Acceptance Tests, Customer may notify Riskconnect during the Acceptance Period. Following notice from Customer, Riskconnect will have a mutually agreed time to remedy the

- deficiencies identified by Customer so that the deliverables satisfy the Acceptance Tests.
- 3.5.2.3.1. Thereafter, if the deficiencies are not remedied to satisfy the Acceptance Tests, the parties may agree to extend the time for Riskconnect to remedy the deficiency in the deliverable and the UAT process will continue until Customer has accepted the deliverable.
- 3.5.2.3.2. If the parties fail to reach agreement on a deliverable, they may escalate the matter to senior management of both parties for resolution and either (A) institute a mutually agreed upon plan to bring the deliverable into acceptance and/or (B) reach an agreement to revise the Statement of Work and modify the project's scope with appropriate adjustments to future fees regarding such deliverable.
- 3.5.2.3.3. If the Parties reach a resolution as described in this section, such resolution shall be Customer's sole and exclusive remedy for any such failure on the part of Riskconnect, and Customer will be deemed to have accepted the deliverable as modified and/or agreed to the project's modified scope.
- 3.5.3. **Project Completion.** With Customer's acceptance and signoff on the project deliverables and promotion of functionality to production environment, the Customer acknowledges the project implementation is complete and will be formally transitioned to their Customer Success team prior to project closure.
- 3.5.3.1. A Project Acceptance Letter will be sent to the Customer on or after the date of go-live. The Customer is requested to sign the Project Acceptance Letter formally closing the project on the date specified in the Project Plan.
- 3.5.3.2. Failure to provide signature or a written reason for dispute within ten (10) business days after production deployment will be deemed as acceptance, and the project will be closed.
- 3.6. **Parties' Responsibilities.** Parties agree to follow the mutually agreed upon Project Plan and the responsibilities listed below:
- 3.6.1. **Data.** County will be responsible for the reasonable timely acquisition of County's Data from County's third-party sources and Riskconnect will be responsible for the design and implementation of data conversions and interfaces. County acknowledges that its failure to accomplish this task in accordance with the Project Plan may result in a negative consequence to the overall implementation schedule and to the implementation budget.
- 3.6.2. **Collaboration**
- 3.6.2.1. County is responsible for ensuring applicable employees are available to provide timely responses to Riskconnect's requests for information and to requests for implementation assistance in accordance with the Project Plan.
- 3.6.2.2. County is responsible for providing Riskconnect information on County's internal processes to the extent applicable to Riskconnect's implementation responsibilities under this Contract.
- 3.6.2.3. County is responsible for performing acceptance testing as set forth in this Contract and the Project Plan.
- 3.6.3. **Approvals.**
- 3.6.3.1. County may need to approve deliverables and/or execute documents (either manually or electronically) before Riskconnect can continue with the implementation project (for example, County may be required to provide acceptance on a task in the Project Plan before Riskconnect can begin another configuration task that is dependent upon the prior task). Such documents shall

solely identify the deliverable or task to be approved; no terms or conditions shall be included in such documents.

3.6.3.2. County must complete User Acceptance Testing and provide signoff prior to production deployment and/or usage in a production environment.

3.7. Project Specifications: Riskconnect Sedgwick Juris Load Interface specifications include the following:

- 3.7.1. Claim Number
- 3.7.2. Status of Claim
- 3.7.3. Clmt Address line 1
- 3.7.4. Clmt Address line 2
- 3.7.5. Clmt Age
- 3.7.6. Clmt first name
- 3.7.7. Clmt last name
- 3.7.8. Clmt middle
- 3.7.9. Clmt state home address
- 3.7.10. Controverted case y/n
- 3.7.11. Date clmt disclosed services of an attorney
- 3.7.12. Date of loss
- 3.7.13. Body part injured
- 3.7.14. Date claim was opened
- 3.7.15. Date claim was reopened after being closed.
- 3.7.16. Date claim was reported to Sedgwick
- 3.7.17. Employee id
- 3.7.18. Reserves only

4. **Out of Scope**

Any Out of Scope services require a PCO amendment to this Contract before such services are performed, and may require an amendment to this Contract as determined by County in its sole discretion. County is not obligated to pay for Out of Scope services performed by Riskconnect that are not added to the Contract via a PCO amendment and, when determined necessary by County, via an amendment.

Out of Scope	
Applications that are not identified in this Contract for which County has a subscription, or any solutions/applications for which County does not have a subscription.	While County has been given access to certain applications via County’s subscription, configuration of applications is limited to only those applications and their provided definitions identified in this Contract. If County decides later that County wants Riskconnect to configure additional applications, this configuration work effort will be handled via a Project Change Order or via a new SOW, which may need to be incorporated into the Contract via an PCO amendment.
Additional Out-of-Scope Items	<ol style="list-style-type: none"> <li>1. Researching, cleaning up and consulting on County Data issues, including reloading County Data due to poor quality</li> <li>2. Revisions to configurations previously approved</li> <li>3. Researching and scoping additional functionality with Development</li> <li>4. Data cleansing and/or manual formatting of any County provided files.</li> <li>5. New County-specified objects (database tables or views) and/or development of any feature that would involve the creation of custom code</li> </ol>

5. **DTPs.**

County data interfaces shall be performed in accordance with Riskconnect’s Data Transfer Protocols, located here: <https://riskconnect.com/legal-dtps/>.



**ATTACHMENT B  
COMPENSATION/COST**

**CONTRACT NOT TO EXCEED AMOUNT: \$571,069.20**

	Year 1	Year 2	Year 3	Year 4	Year 5
<b>ANNUAL MAX NOT TO EXCEED AMOUNT</b>	\$130,413.84	\$110,163.84	\$110,163.84	\$110,163.84	\$110,163.84

1. **COMPENSATION:** This is a fixed price Contract between County and Riskconnect for the Services as set forth in this Contract. Riskconnect agrees to supply all Services as set forth in this Contract. Riskconnect agrees to accept the specified compensation as set forth in this Contract in accordance with any Subscription Order or Statement of Work, which shall be subject to the terms and conditions of this Contract.

County shall have no obligation to pay any sum in excess of the amounts specified herein unless authorized by an amendment.

In the tables below, "Year" shall be defined as the twelve (12) months from the Effective Date of the Contract.

2. **FEES – ATTACHMENT A (SCOPE OF SERVICES-SUBSCRIPTION ORDER)**

Following the Effective Date and on each anniversary of the Effective Date thereafter during the Term, and following receipt of an acceptable invoice from Riskconnect, County will pay in advance the following annual fees for the performance of Attachment A (Scope of Services).

**2.1. SERVICES FEES - MAINTENANCE LIABILITY 294**

Item	Services Description	Units	Year 1 Flat Fee	Year 2 Flat Fee	Year 3 Flat Fee	Year 4 Flat Fee	Year 5 Flat Fee	Year 6* Flat Fee*	Year 7* Flat Fee*
01	Admin Users – RMIS	1	\$8,400.00	\$8,400.00	\$8,400.00	\$8,400.00	\$8,400.00	\$8652.00	\$8911.56
02	Full Users	7	\$31,850.00	\$31,850.00	\$31,850.00	\$31,850.00	\$31,850.00	\$32,805.50	\$33,789.67
03	Operations W/Reports	4	\$1,458.00	\$1,458.00	\$1,458.00	\$1,458.00	\$1,458.00	\$1,501.74	\$1,546.79
04	Operations	7	\$1,841.00	\$1,841.00	\$1,841.00	\$1,841.00	\$1,841.00	\$1,896.23	\$1,953.12
05	Business Insights Adv.	1	\$1,370.00	\$1,370.00	\$1,370.00	\$1,370.00	\$1,370.00	\$1,411.10	\$1,453.43
06	eComposer	10	\$3,000.00	\$3,000.00	\$3,000.00	\$3,000.00	\$3,000.00	\$3,090.00	\$3,182.70

\*Payment of Year 6 and Year 7 fees is contingent upon, and requires an amendment for, renewal of this Contract. If the Contract is not renewed for Year 6 and/or Year 7, County shall not pay the amounts listed in Year 6 and/or Year 7.

**2.2. STORAGE SUBSCRIPTION FEES**

Item	Services Description	Units	Year 1 Flat Fee	Year 2 Flat Fee	Year 3 Flat Fee	Year 4 Flat Fee	Year 5 Flat Fee	Year 6* Flat Fee*	Year 7* Flat Fee*
01	Riskconnect Infrastructure (Data)	2	\$8,500.00	\$8,500.00	\$8,500.00	\$8,500.00	\$8,500.00	\$8,755.00	\$9,017.65
02	File Add-On	50	\$6,000.00	\$6,000.00	\$6,000.00	\$6,000.00	\$6,000.00	\$6,180.00	\$6,365.40

\*Payment of Year 6 and Year 7 fees is contingent upon, and requires an amendment for, renewal of this Contract. If the Contract is not renewed for Year 6 and/or Year 7, County shall not pay the amounts listed in Year 6 and/or Year 7.

**2.3. DATA SUBSCRIPTION AND LICENSES FEES**

Item	Service Description	Units	Year 1 Flat Fee	Year 2 Flat Fee	Year 3 Flat Fee	Year 4 Flat Fee	Year 5 Flat Fee	Year 6* Flat Fee*	Year 7* Flat Fee*
01	Annual Customer Support Hours	34	\$6,375.00	\$6,375.00	\$6,375.00	\$6,375.00	\$6,375.00	\$6,566.25	\$6,763.24
02	<b>Data Subscription:</b> CAPS+, Inbound Daily	---	\$7,500.00	\$7,500.00	\$7,500.00	\$7,500.00	\$7,500.00	\$7,725.00	\$7,956.75

03	ISO Query, Bi-Direct	---	\$3,500.00	\$3,500.00	\$3,500.00	\$3,500.00	\$3,500.00	\$3,605.00	\$3,713.15
04	ISO Center for Medicare, Bi-Direct Daily	---	\$3,500.00	\$3,500.00	\$3,500.00	\$3,500.00	\$3,500.00	\$3,605.00	\$3,713.15

\*Payment of Year 6 and Year 7 fees is contingent upon, and requires an amendment for, renewal of this Contract. If the Contract is not renewed for Year 6 and/or Year 7, County shall not pay the amounts listed in Year 6 and/or Year 7.

**2.4. TOTAL ANNUAL FEES – ATTACHMENT A (2.1, 2.2 and 2.3 Totals)**

Item	Service Description	Year 1 Flat Fee	Year 2 Flat Fee	Year 3 Flat Fee	Year 4 Flat Fee	Year 5 Flat Fee	Year 6* Flat Fee*	Year 7* Flat Fee*
01	Total Annual Fees	\$83,294.00	\$83,294.00	\$83,294.00	\$83,294.00	\$83,294.00	\$85,792.82	\$88,366.61

\* Payment of Year 6 and Year 7 fees is contingent upon, and requires an amendment for, renewal of this Contract. If the Contract is not renewed for Year 6 and/or Year 7, County shall not pay the amounts listed in Year 6 and/or Year 7.

**3. FEES – ATTACHMENT A-1 (ADDITIONAL SCOPE OF SERVICES)**

3.1. **Following** the Effective Date and on each anniversary of the Effective Date thereafter during the Term, following receipt of an acceptable invoice from Riskconnect, County will pay in advance the following annual fees for the performance of Attachment A-1 (Additional Scope of Services).

Item	Service Description	Units	Year 1 Flat Fee	Year 2 Flat Fee	Year 3 Flat Fee	Year 4 Flat Fee	Year 5 Flat Fee	Year 6* Flat Fee*	Year 7* Flat Fee*
01	File Storage – Add on	50	\$6,000.00	\$6,000.00	\$6,000.00	\$6,000.00	\$6,000.00	\$6,180.00	\$6,365.40
Item	SEDGWICK JURIS INBOUND FEED	Units	Year 1 Flat Fee	Year 2 Flat Fee	Year 3 Flat Fee	Year 4 Flat Fee	Year 5 Flat Fee	Year 6* Flat Fee*	Year 7* Flat Fee*
01	Configuration	---	None	None	None	None	None	None	None
02	Annual FEES Role Based User	1	\$600.00	\$600.00	\$600.00	\$600.00	\$600.00	\$618.00	\$636.54
03	On-Going Data Semi Monthly	1	\$4,750.00	\$4,750.00	\$4,750.00	\$4,750.00	\$4,750.00	\$4,892.50	\$5,039.28
	<b>NEW SERVICE FEES</b>	---	<b>\$11,350.00</b>	<b>\$11,350.00</b>	<b>\$11,350.00</b>	<b>\$11,350.00</b>	<b>\$11,350.00</b>	<b>\$11,690.50</b>	<b>\$12,041.22</b>

\*Payment of Year 6 and Year 7 fees is contingent upon, and requires an amendment for, renewal of this Contract. If the Contract is not renewed for Year 6 and/or Year 7, County shall not pay the amounts listed in Year 6 and/or Year 7.

**3.2. IMPLEMENTATION FEES – ATTACHMENT A-1**

Upon execution of the Contract and start of implementation, Contractor may invoice County for 50% of the total Implementation Fees noted in the table below. Contractor then shall invoice County the remaining 50% of the total implementation fees in arrears at completion of project (Go-Live). Payment will be based on actual hours worked, with justification for the hours billed included with the invoice.

Item	Service Description	Units	Year 1 Flat Fee	Year 2 Flat Fee	Year 3 Flat Fee	Year 4 Flat Fee	Year 5 Flat Fee	Year 6* Flat Fee*	Year 7* Flat Fee*
01	Implementation Fees Professional Hours	108	\$20,250.00	None	None	None	None	None	None

**3.3. TOTAL FEES FOR ATTACHMENT A-1 SERVICES (3.1 AND 3.2 TOTALS)**

Item	Service Description	Year 1 Flat Fee	Year 2 Flat Fee	Year 3 Flat Fee	Year 4 Flat Fee	Year 5 Flat Fee	Year 6* Flat Fee*	Year 7* Flat Fee*
	<b>NEW SERVICE FEES</b>	<b>\$31,600.00</b>	<b>\$11,350.00</b>	<b>\$11,350.00</b>	<b>\$11,350.00</b>	<b>\$11,350.00</b>	<b>\$11,690.50</b>	<b>\$12,041.22</b>

\*Payment of Year 6 and Year 7 fees is contingent upon, and requires an amendment for, renewal of this Contract. If the Contract is not renewed for Year 6 and/or Year 7, County shall not pay the amounts listed in Year 6 and/or Year 7.

**4. GRAND TOTAL FOR ATTACHMENT A AND ATTACHMENT A-1 SERVICES\*\***

4.1. The grand total amount under this Contract for Attachment A and Attachment A-1 Services is:

Item	Service Description	Year 1 Flat Fee	Year 2 Flat Fee	Year 3 Flat Fee	Year 4 Flat Fee	Year 5 Flat Fee	Year 6* Flat Fee*	Year 7* Flat Fee*
01	GRAND TOTAL	\$114,894.00	\$96,644.00	\$96,444.00	\$96,444.00	\$96,444.00	\$97,483.32	\$100,407.82

\*Payment of Year 6 and Year 7 fees is contingent upon, and requires an amendment for, renewal of this Contract. If the Contract is not renewed for Year 6 and/or Year 7, County shall not pay the amounts listed in Year 6 and/or Year 7.

**\*\*Optional Additional Service costs are not included in the “Grand Total” due to Contractor. Contractor may bill for the optional additional services separately as needed and approved by County in accordance with the terms of this Contract; provided, however, that Contractor shall not provide optional additional services that would exceed the Contract’s not to exceed amounts.**

## 5. OPTIONAL ADDITIONAL SERVICES AND COST

5.1 At its option, County may add the following additional services as needed and requested in writing by County, up to the Contract’s Not to Exceed Amount.

5.1.1 RCMIS Licenses: County may add RCMIS licenses up to the maximum amount noted below at the following pre-negotiated costs.

User License Type	Max Additional Available	Price per Unit
Platform Administrative Users (RCMIS)	2	\$8,400
Platform Full Users	5	\$4,550
Operations Users (with Reports)	10	\$360
Operations Users	10	\$263
Riskconnect Business Intelligence Report Studio	3	\$2,630
Riskconnect Business Intelligence Business Insights Advanced	5	\$1,370
Riskconnect Business Intelligence Report Consumer	5	\$840

5.1.2 Data Storage: County may add data storage at the following pre-negotiated cost.

5.1.2.1 Contractor shall notify County when County is close to reaching and when County has reached the maximum amount of data or file storage subscribed by County in Table 3.1 and Table 2.2 of this Attachment B. If County exceeds the maximum amount, County shall reduce its data storage to the amount subscribed or shall pay excess data storage fees at the following pre-negotiated costs.

Storage Type	Annual Price per unit (per Gigabyte)
Record (data) storage	\$2,500
Attachment storage fee	\$120

5.2 Data Feeds: County may add the following data feeds at the following pre-negotiated costs:

Interface Name	Inbound/Outbound or Bi-Directional	Transmission type	Frequency	One-Time Cost	Annual Cost
CAPS+	Bi-Directional	SFTP	One-Time	\$5,000	
CAPS+	Bi-Directional	SFTP	Daily		\$7,500
CAPS+	Bi-Directional	SFTP	Weekly		\$5,000
CAPS+	Bi-Directional	SFTP	Monthly		\$4,000
Identity Management	Inbound	SFTP	Daily	\$1,500	\$3,500

5.3 Professional Support Services: County may add Professional Support Services substantially related to the professional services provided under this Contract. County will request Professional Support Services in writing and the Riskconnect project manager will provide County a reasonable estimate on the number of hours needed to complete the requested professional support services. If County approves the Professional

Support Services in writing, Contractor must invoice County for such hours monthly at the hourly rate noted in the table below.

Professional Services Support	Hourly Rate
Up to an additional 50 hours annually	\$200

## 6 COUNTY PAYMENT TERMS

Riskconnect shall reference Contract # MA-017-22010011 on every invoice. Payment will be net 45 days, unless otherwise stated, after receipt of an invoice in a format acceptable to the County and verified and approved by the agency/department and subject to routine processing requirements. The responsibility for providing an acceptable invoice rest with Riskconnect. Incomplete or incorrect invoices are not acceptable and will be returned to Riskconnect for correction. The County's Project Manager, or designee, is responsible for approval of invoices and subsequent submittal of invoices to the Auditor-Controller for processing of payment.

Billing shall cover services and/or goods not previously invoiced. Riskconnect shall reimburse the County for any monies paid to Riskconnect for goods or services not provided or when goods or services do not meet the Contract requirements.

Payments made by the County shall not preclude the right of the County from thereafter disputing any items or services involved or billed under this Contract and shall not be construed as acceptance of any part of the goods or services.

## 7 PAYMENT/INVOICING INSTRUCTIONS

Riskconnect will provide an invoice on Riskconnect's letterhead for services rendered. Each invoice will have a number and will include the following information:

- a. Riskconnect's name and address
- b. Riskconnect's remittance address (if different from (a.) above)
- c. Name of County agency department
- d. County Contract number
- e. Service date(s)
- f. Service description
- g. Riskconnect's Federal I. D. number
- h. Total

## 8 E-INVOICES AND SUPPORT DOCUMENTATION MUST BE FORWARDED TO:

County of Orange  
 Risk Management Office  
 Attn: Risk Management Director  
 601 N. Ross Street, 5<sup>th</sup> Floor  
 Santa Ana, CA 92701-7530

- 9 **ELECTRONIC FUNDS TRANSFER (EFT):** County of Orange offers Contractors the option to receive direct payment to their bank account via an Electronic Fund Transfer (EFT) process in lieu of a check payment. Payment made via EFT will also receive an Electronic Remittance Advice with the payment details via e-mail. To request an EFT form, please contact DPA.



## ATTACHMENT C

### RISKONNECT SECURITY AND SERVICE LEVELS

1. “Platform Provider” in this Attachment C means Salesforce (force.com).
2. “Analytics and Data Aggregation Environment” or “ADI” in this Attachment C means Rackspace.

Standard	What Riskonnect does
<b>Regulated Data Security Controls</b>	<b>Riskonnect Platform:</b> SSAE18 Type2, SOC2 Type2; PCI; HIPAA HITECH
	<b>Xactium Platform:</b> ISO27001
	<b>Riskonnect/Xactium Platform Provider:</b> SSAE18 Type2, SOC2 Type2; HIPAA HITECH; PCI. Additional Platform certifications can be found at trust.salesforce.com.
	<b>Riskonnect Analytics and Data Aggregation Environment:</b> SSAE18 Type2, SOC2 Type2; PCI
	<b>Clearsight Platform:</b> SSAE18 Type2.
<b>Patching</b>	<b>Riskonnect/Xactium Platform Provider:</b> Patches are remediated based on Riskonnect/Xactium Platform Provider’s Patch Management Document which can be provided upon request.
	<b>Riskonnect Analytics and Data Aggregation Environment:</b> Riskonnect patches its infrastructure within 30 days for all patches and hot fixes following Riskonnect’s change control policy. Riskonnect can apply emergency patches as necessary if the vulnerability warrants immediate remediation.
	<b>Clearsight Platform:</b> <b>Infrastructure excluding database application:</b> Riskonnect will patch the ClearSight infrastructure within 30 days for all patches and hotfixes following Riskonnect’s change control policy. Riskonnect can apply emergency patches as necessary if the vulnerability warrants immediate remediation
	<b>Application:</b> Riskonnect will patch the ClearSight application based on the following schedule: Critical application issue - within 14 days of identification High - within 30 days of identification Medium - within 60 days of identification Low - Evaluated per major release.
	<b>Database:</b> Riskonnect will patch the Oracle database software within 6-8 weeks after an official Oracle PSU is released following our change control policy.
	<b>All:</b> Riskonnect reserves the right to apply emergency patches to any portion of our infrastructure or application as necessary to mitigate or remediate a critical vulnerability if one is identified. In all instances, Tech Ops would follow the Riskonnect change control policy.
	<b>Vulnerability Management</b>
	<b>Riskonnect Analytics and Data Aggregation Environment:</b> Riskonnect performs quarterly infrastructure vulnerability scans (internal and external port scans). In addition, Riskonnect engages a third party to perform an infrastructure vulnerability scan annually. Riskonnect follows the below remediation timeline:
	<b>Vulnerability Risk Rating (based on the common vulnerability scoring system)</b>
	<b>Remediation Timeframe</b>

	<b>Critical</b>	No later than 7 days after the vulnerability is identified.
	<b>High</b>	No later than 30 days after the vulnerability is identified.
	<b>Medium</b>	No later than 90 days after the vulnerability is identified.
	<b>Low/Informational</b>	As appropriate
<b>ClearSight Platform:</b>		
<b>Infrastructure:</b> Riskconnect engages a third party to perform a quarterly external infrastructure vulnerability scan. Riskconnect follows the below remediation timeline:		
	<b>Vulnerability Risk Rating (based on the common vulnerability scoring system)</b>	<b>Remediation Timeframe</b>
	<b>Critical</b>	No later than 7 days after the vulnerability is identified.
	<b>High</b>	No later than 30 days after the vulnerability is identified.
	<b>Medium</b>	No later than 90 days after the vulnerability is identified.
	<b>Low/Informational</b>	As appropriate.
<b>Application:</b>		
Riskconnect will patch the ClearSight application based on the following schedule:		
	<b>Vulnerability Risk Rating (based on the common vulnerability scoring system)</b>	<b>Remediation Timeframe</b>
	<b>Critical</b>	No later than 7 days after the vulnerability is identified.
	<b>High</b>	No later than 30 days after the vulnerability is identified.
	<b>Medium</b>	No later than 90 days after the vulnerability is identified.
	<b>Low/Informational</b>	As appropriate.
<b>Encryption at Rest</b>	<b>Riskconnect/Xactium Platform Provider:</b> Platform encryption is not standard. Platform field-based encryption is available for an additional cost. Once purchased, Customer is able to manage the tenant secret used for encryption and decryption tasks.	
	<b>Riskconnect Analytics and Data Aggregation Environment:</b> Currently all Customer data that resides in Riskconnect’s data aggregation environment is encrypted utilizing container-based encryption. All directories where Customer data is stored and encrypted using transparent data encryption. Riskconnect manages these keys	
	<b>ClearSight Platform:</b> All data that resides in the ClearSight platform is encrypted utilizing hardware appliance-based encryption. Riskconnect manages these keys.	
<b>Firewall</b>	<b>Riskconnect/Xactium Platform Provider:</b> Perimeter firewalls and edge routers are used to block unused transmission protocols, and internal firewalls are used to segregate traffic between the application and database tiers	
	<b>Riskconnect Analytics and Data Aggregation Environment:</b> A firewall exists in our infrastructure which allows for multi-zone network segmentation between DMZ and internal network segments. This firewall is managed by Riskconnect Technical Operations.	
	<b>ClearSight Platform:</b> Perimeter firewalls and edge routers are used to block unused transmission protocols, and internal firewalls are used to segregate traffic between the application and database tiers.	

<b>Malware Protection</b>	<b>Riskconnect/Xactium Platform Provider:</b> Riskconnect's Platform Provider runs antivirus software on the production systems, which scans host filesystems (not Customer data). Definitions are updated daily.
	<b>Riskconnect Analytics and Data Aggregation Environment:</b> All endpoints and servers have Anti-Virus software installed and enabled. Scanning is performed in real-time. Definitions are updated daily.
	<b>ClearSight Platform:</b> All endpoints and servers have Anti-Virus software installed and enabled. Scanning is performed in real-time. Definitions are updated daily.
<b>Backups</b>	<b>Riskconnect/Xactium Platform Provider:</b> The Riskconnect service provides real time replication to disk and near real time replication between the primary data center and the secondary data center. Backups occur over encrypted connections between servers, but are not encrypted at rest.
	<b>Riskconnect Analytics and Data Aggregation Environment:</b> Backups are done using the following schedule: <ul style="list-style-type: none"> <li>• Daily - Differential backup, all systems.</li> <li>• Weekly - Full backup, all systems</li> </ul>
	Backups are stored using the following schedule: <ul style="list-style-type: none"> <li>• Production Systems - 4 weeks offsite.</li> <li>• All other systems - 2 week onsite.</li> </ul>
	All backups are encrypted.
	<b>ClearSight Platform:</b>
	<b>Database:</b> Backups are done using the following schedule: Block level backup - near real time replication between the primary data center and the secondary data center.
	<b>RMAN Backup:</b> Backups are done using the following schedule: <ul style="list-style-type: none"> <li>• Weekly - full backup.</li> <li>• Daily - incremental (2-week onsite retention.)</li> </ul>
	<b>OS for DB Server:</b> Backups are done using the following schedule: <ul style="list-style-type: none"> <li>• Weekly - full backup.</li> <li>• Daily – incremental.</li> </ul> Backups are stored onsite in the primary data center and replicated to the secondary data center. Backup is encrypted using AES256.
	<b>US Fileshare Backups:</b> Backups are done using the following schedule: <ul style="list-style-type: none"> <li>• Weekly - full backup.</li> <li>• Daily – incremental.</li> </ul> All backups replicated to the secondary data center. Backups encrypted using AES 256.
	<b>UK Fileshare Backups:</b> Backups are done using the following schedule: <ul style="list-style-type: none"> <li>• Weekly - full backup.</li> <li>• Daily – incremental.</li> </ul> All backups replicated to the secondary data center. Backups encrypted using AES 256
<b>Inventory</b>	<b>Riskconnect/Xactium Platform Provider:</b> Physical inventories of all production systems that reflect the current information system environment are documented and the inventories are maintained for tracking and reporting purposes. A physical inventory of production systems is performed periodically.

	<p><b>Riskconnect Analytics and Data Aggregation Environment:</b> All hardware and software owned by Riskconnect is entered into an Asset Inventory system inside of the Riskconnect CRM. Every asset has an owner that is entered into the asset record.</p> <p><b>ClearSight Platform:</b> All hardware and software owned by Riskconnect is entered into an Asset Inventory system. Every asset has an owner that is entered into the asset record.</p>
<b>Credentials and Access Control</b>	<p><b>Riskconnect/Xactium Platform Provider:</b> Admin credentials and access control used by Riskconnect to provide service and support to customers are reviewed regularly by the Riskconnect Technical Operations Team.</p>
	<p><b>Riskconnect Analytics and Data Aggregation Environment:</b> Credentials and Access Control are reviewed regularly by the Riskconnect Technical Operations Team.</p>
	<p><b>ClearSight Platform:</b> Admin credentials and access control used by Riskconnect to provide service and support to customers are reviewed regularly by the Riskconnect Technical Operations team.</p>
<b>Two-Factor Authentication</b>	Riskconnect utilizes two-factor authentication for access to all systems including access to Customer Orgs, email infrastructure, and internal systems.
<b>Centralized Logging</b>	<p><b>Riskconnect/Xactium Platform Provider:</b> Automated, read-only audit trails are implemented and collected in the system for Customer Admins to review as needed. Logs are kept on a 6-month rolling cycle. Logs can be extracted by Customer and imported into Customer's SIEM software for further analysis as required.</p>
	<p><b>Riskconnect Analytics and Data Aggregation Environment:</b> All log data from internal systems are collected in Riskconnect's log aggregation software. Alerts are setup for critical threshold events which can be addressed by Riskconnect Technical Operations.</p>
	<p><b>ClearSight Platform:</b> Application logs are available to users within the platform for audit reporting purposes as required.</p> <p>All log data from internal systems are collected in Riskconnect's log aggregation software. Alerts are setup for critical threshold events which can be addressed by Riskconnect Technical Operations.</p>
<b>Intrusion Detection</b>	<p><b>Riskconnect/Xactium Platform Provider:</b> Intrusion detection system (IDS) is in place to monitor for potential security events, and the monitoring system is configured to distribute alerts as events occur. All event monitoring is done by Salesforce.com's Trust Security Organization.</p>
	<p><b>Riskconnect Analytics and Data Aggregation Environment:</b> IDS is in place to monitor for potential security events, and the monitoring system is configured to distribute alerts as events occur. The event data is distributed to Riskconnect Technical Operations to act on and resolve.</p>
	<p><b>ClearSight Platform:</b> IPS/WAF is in place to monitor for potential security events, and the monitoring system is configured to distribute alerts as events occur. The event data is distributed to Riskconnect Technical Operations to act on and resolve</p>
<b>Physical Protection</b>	<p><b>Riskconnect/Xactium Platform Provider:</b> Physical access controls, including badge readers, biometric devices, and security guards limit access to facilities and designated services areas to authorized personnel. A biometric access control system is in place at each of the data center facilities for restricted or secured areas and linked to an alarm system. Multiple two-factor authentication checkpoints are in place. Visitor policies are in place and are strictly enforced.</p>

	<p><b>Riskconnect Analytics and Data Aggregation Environment:</b> Controlled building access and secure access to specific areas are enforced through the administration of badges/cards and biometric devices. Access to the data center is restricted through the use of biometric authentication devices and key-card-badge devices. Two-factor authentication is used to gain access to the data center and access is restricted to only authorized personnel. Visitor policies are in place and are strictly enforced.</p> <p><b>ClearSight Platform:</b> Controlled building access and secure access to specific areas are enforced through the administration of badges/cards and biometric devices. Access to the data center is restricted through the use of biometric authentication devices and key-card-badge devices. Two-factor authentication is used to gain access to the data center and access is restricted to only authorized personnel. Visitor policies are in place and are strictly enforced.</p>
<b>Configuration Management</b>	<p><b>Riskconnect/Xactium Platform Provider:</b> An internal configuration management process that follows the Platform Provider's change control policy is in place.</p>
	<p><b>Riskconnect Analytics and Data Aggregation Environment:</b> All changes that occur within Riskconnect's ADI environment follow Riskconnect's change control policy. The change control policy is part of Riskconnect's IS Policies and Procedures.</p>
	<p><b>ClearSight Platform:</b> An automated tool is used to configure hardware and software used within the platform. This tool uses baseline configurations as well as iterative software manifests to consistently push patches and application upgrades across the entire infrastructure.</p>
<b>Incident Response Times</b>	In the event of a confirmed security incident, Riskconnect will follow our Incident Response Plan, and customers will be notified within 48 hours of Riskconnect's knowledge of the incident.

### 3. SERVICE LEVELS

The service level metrics described herein shall be measured quarterly after implementation of the Riskconnect Service.

#### **Availability**

The Riskconnect Service delivered via the Platform Service shall be available to Users at least 99.7% of the time measured on a quarterly basis for the 3-month period ending on the last day of each calendar quarter. Availability of the Riskconnect Service is monitored and measured by Riskconnect in Customer's production environment.

Availability will be calculated based on the following calculation:

$$\frac{\text{(Service Cover Time – Unavailability)}}{\text{Service Cover Time}} \times 100$$

“Service Cover Time” - Total number of minutes in a calendar quarter.

“Unavailability” - Total number of minutes in any calendar quarter during which functionality of the service is subject to a Service Affecting Fault other than any Exceptions to Unavailability.

“Service Affecting Fault” - Service is completely unavailable or day-to-day business is severely impacted and the cause is not the result of any Exceptions to Unavailability. The following are not Service Affecting Faults: Any reported fault where (i) the Customer's ability to use components of the Riskconnect Service to perform work is moderately impacted and day-to-day business may suffer some impact; or (ii) one or more business applications are unable to operate fully but the Customer can carry out most or all of their daily tasks with minimal or no major impact on the day-to-day business; and (iii) all applications can be used but some features are affected but the causes are not the result of any of the Exceptions to Unavailability.

“Exceptions to Unavailability” - Maintenance, any loss of service that is the result of the Customer (network access, configuration, firewall limits, etc.), any loss due to a force majeure event, or any loss due to a third party application integrated at Customer's request, including:



- scheduled maintenance,
- emergency maintenance,
- any other agreed-to scheduled downtime activity,
- upgrade maintenance window from Riskconnect or its platform hosting provider, salesforce.com,
- any unavailability to Users due to outages elsewhere in the internet or due to connectivity issues from ISP (internet service provider),
- browser issues,
- DNS and/or any caching that may make User accounts look inaccessible, or
- any unavailability caused by circumstances beyond Riskconnect's reasonable control, including without limitation, acts of God, shortages of supplies, labor or materials, strikes and other labor disputes, storms, floods, acts of war or terrorism, failure of third-party hardware, software, services or networks, failure of service providers, utility blackouts or brownouts, failure of telecommunications or the internet, and actions by a governmental authority (such as changes in government codes, ordinances, laws, rules, regulations, or restrictions).

## Software Support

Severity	Definition	Acknowledgement Timing	Action Plan	Communication Frequency
Urgent - 1	All Users are unable to access the Riskconnect Service or are unable to access one or more critical functions of the Riskconnect Service, and no immediate workaround exists. ==Or== Customer will face regulatory fines within next 3 business days if a resolution to the incident is not found.	1 Absolute Hour.	4 Subsequent Absolute Hours.	Every Subsequent 4 Absolute Hours.
High - 2	Non-critical major function(s) or feature(s) of the Riskconnect Service is (are) inhibited for a set of Users. == Or == a critical function is failing with a known workaround.	2 Business Hours.	6 Subsequent Business Hours.	Every Subsequent 8 Business Hours.
Medium - 3	There is an incident to be resolved on a non-critical function but the Riskconnect Service is still functional and Users have other options available.	8 Business Hours.	N/A	N/A
Low - 4	Minor issues with the Riskconnect Service with no impact to the ability of Users to perform their normal duties. ==Or== Incident is cosmetic in nature.	16 Business Hours.	N/A	N/A

Definitions and Restrictions	
Contact Channels	<p>For SLA calculation purposes, all support incidents must have a case reference number. All Severity 1 issues must be submitted by an authorized representative of Customer, via telephone, to the Riskconnect Support Call Center at +1.855.478.2771.</p> <p>Severity 2, 3, or 4 issues may be submitted via:</p> <ul style="list-style-type: none"> <li>• Phone call to Riskconnect Support Call Center at +1.855.478.2771.</li> <li>• email-to-case: help.me@riskconnect.com</li> <li>• Web-based case management system accessible via the Riskconnect Service.</li> </ul>
What is the scope of Software Support?	<p>Software Support is defined as Riskconnect's effort to diagnose and resolve incidents or faults when the production system is not operating as documented or as it has operated in the past.</p> <p>Software Support usually includes, but is not limited to the following types of incidents:</p> <ul style="list-style-type: none"> <li>• New Error message troubleshooting.</li> </ul>

	<ul style="list-style-type: none"> <li>• System Access/login issues.</li> <li>• Performance Issues.</li> <li>• Unexpected results.</li> <li>• "Break-Fix" situations.</li> </ul> <p>Software Support does <u>not</u> include:</p> <ul style="list-style-type: none"> <li>• Setup (New Workflow) Error message troubleshooting.</li> <li>• Service Requests.</li> <li>• Configuration requests.</li> <li>• Change Requests.</li> <li>• Enhancement / New Feature requests.</li> <li>• Consulting Requests.</li> <li>• Customer-side Development assistance.</li> <li>• Customer-side infrastructure or workstation configuration.</li> </ul>
Hours Calculation	<p>Absolute Hours:</p> <ul style="list-style-type: none"> <li>• 60 consecutive minutes;</li> <li>• Calculated on a 24-hour clock;</li> <li>• One Absolute Day is 24 hours.</li> </ul> <p>Business Hours:</p> <ul style="list-style-type: none"> <li>• Determined based on the region of the Customer User desiring Software Support;</li> <li>• One Business Day is a maximum of 8 hours;</li> <li>• Starting at 08:00 Regional Time.</li> <li>• Excluding official holidays in the Customer User's nation, state, or province.</li> </ul> <p>Regional Time is:</p> <ul style="list-style-type: none"> <li>• Americas: Monday - Friday 08:00-17:00 CST/CDT</li> <li>• APAC: Monday - Friday 08:00-16:00 AEST/AEDT</li> <li>• EU: Monday - Friday 08:00 - 17:00 GMT/BST.</li> </ul>
Defects and Code Changes	<p>Software Support incidents requiring a change to the shared codebase or a complex change to custom code are promoted to the classification of "Defect."</p> <p>At the point when a support incident is determined to be the result of a Defect, then the Software Support Action Plan and Communication Frequency metrics shall no longer apply, but shall be separately set forth in the Action Plan. Defect prioritization is then performed by Riskconnect based on severity and on the quantity of affected customers.</p>
Suspension	<p>Upon documented mutual agreement between Riskconnect and Customer, the communications frequency for a particular incident may be suspended until a defined future point in time.</p>
Environment	<p>This Software Support SLA only applies solely to the Customer's primary production environment. Customers may have access to other environments that are not subject to this Software Support SLA, including but not limited to: UAT, pre-production, stage, test, or other non-production environments.</p>

## ATTACHMENT D

### HIPAA BUSINESS ASSOCIATE AGREEMENT

#### 1 HIPAA Compliance

Subject to the terms and conditions of the Contract Riskconnect agrees to comply with all requirements that are now or will become applicable to it in its role as the service provider under this Contract pursuant to regulations issued pursuant to 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 may exist now or be hereafter amended . Further to Riskconnect’s obligations hereunder, Riskconnect shall comply with the requirements set forth below.

#### 2 Business Associate

##### 2.1 General Provisions and Recitals

- a. The Parties agree that the terms used, but not otherwise defined below in Section 2.2, 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 may exist now or be hereafter amended.
- b. The Parties agree that a business associate relationship under HIPAA, the HITECH Act, and the HIPAA regulations between the Riskconnect and County arises to the extent that Contractor performs, or delegates to subcontractors to perform, functions or activities on behalf of County pursuant to, and as set forth in, this Contract that are described in the definition of “Business Associate” in 45 CFR § 160.103.
- c. The County wishes to disclose to Riskconnect certain information pursuant to the terms of this Contract, some of which may constitute Protected Health Information (“PHI”), as defined below in Section 2.2(j), to be used or disclosed in the course of providing services and activities pursuant to, and as set forth, in this Contract.
- d. 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 this Contract in compliance with the applicable standards, implementation specifications, and requirements of HIPAA, the HITECH Act, and the HIPAA regulations as they may exist now or be hereafter amended.
- e. 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 are not otherwise pre-empted by other Federal law(s) and impose more stringent requirements with respect to privacy of PHI.
- f. The Parties understand that the HIPAA Privacy and Security rules, as defined below in Section 2.2(i) and (n), apply to the Riskconnect in the same manner as they apply to a covered entity (County). Riskconnect agrees therefore to be in compliance at all times with the terms of this Contract and the applicable standards, implementation specifications, and requirements of the Privacy and the Security rules, as they may exist now or be hereafter amended, with respect to PHI and electronic PHI created, received, maintained, transmitted, used, or disclosed pursuant to this Contract.
- g. The Parties agree to take such action as is necessary to amend this Contract from time to time as is necessary for the County to comply with the requirements of the HIPAA, the HITECH Act and applicable regulations.

##### 2.2 Definitions

The following definitions apply only to this Attachment H and all other references to HIPAA in this

Contract. All of definitions shall be as otherwise specified in this Contract.

- A. “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 Riskconnect’s workforce in relation to the protection of that information.
- B. “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.
- i. Breach excludes:
- a. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of Riskconnect or County, 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.
  - b. Any inadvertent disclosure by a person who is authorized to access PHI at Riskconnect to another person authorized to access PHI at the RISKCONNECT, or organized health care arrangement in which County participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule.
  - c. A disclosure of PHI where Riskconnect or County 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.
- ii. Except as provided in paragraph (i) of this Section 2.2, 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 Riskconnect 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.
- C. “Data Aggregation” shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR § 164.501.
- D. “Designated Record Set” shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR § 164.501.
- E. “Disclosure” shall have the meaning given to such term under the HIPAA regulations in 45 CFR § 160.103.
- F. “Health Care Operations” shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR § 164.501.
- G. “Individual” shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).
- H. “Physical Safeguards” are physical measures, policies, and procedures to protect Riskconnect’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.
- I. “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.



- J. “Protected Health Information” or “PHI” shall have the meaning given to such term under the HIPAA regulations in 45 CFR § 160.103.
- K. “Required by Law” shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR § 164.103.
- L. “Secretary” shall mean the Secretary of the Department of Health and Human Services or his or her designee.
- M. “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 Riskconnect.
- N. “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.
- O. “Subcontractor” shall have the meaning given to such term under the HIPAA regulations in 45 CFR § 160.103.
- P. “Technical safeguards” means the technology and the policy and procedures for its use that protect electronic PHI and control access to it.
- Q. “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 in the guidance issued on the HHS Web site.
- R. “Use” shall have the meaning given to such term under the HIPAA regulations in 45 CFR § 160.103.

### 2.3 Obligations and Activities of Riskconnect as Business Associate

- A. Riskconnect agrees not to use or further disclose PHI County discloses to Riskconnect other than as permitted or required by this Business Association Agreement or as required by law.
- B. Riskconnect agrees to use appropriate safeguards, as provided for in this Business Associate Agreement and this Contract, to prevent use or disclosure of PHI County discloses to Riskconnect or Riskconnect creates, receives, maintains, or transmits on behalf of County other than as provided for by this Business Associate Agreement.
- C. Riskconnect agrees to comply with the HIPAA Security Rule at Subpart C of 45 CFR Part 164 with respect to electronic PHI County discloses to Riskconnect or Riskconnect creates, receives, maintains, or transmits on behalf of County.
- D. Riskconnect agrees to mitigate, to the extent practicable, any harmful effect that is known to Riskconnect of a Use or Disclosure of PHI by Riskconnect in violation of the requirements of this Business Associate Agreement.
- E. Riskconnect agrees to report to County immediately any Use or Disclosure of PHI not provided for by this Business Associate Agreement of which Riskconnect becomes aware. Riskconnect must report Breaches of Unsecured PHI in accordance with Section 2.5 below and as required by 45 CFR § 164.410.
- F. Riskconnect agrees to ensure that any Subcontractors that create, receive, maintain, or transmit PHI on behalf of Riskconnect agree to the same restrictions and conditions that apply through this Contract to Riskconnect with respect to such information.
- G. Riskconnect agrees to provide access, within fifteen (15) calendar days of receipt of a written request by County, to PHI in a Designated Record Set, to County or, as directed by County, to an Individual in order to meet the requirements under 45 CFR § 164.524.

- H. Riskconnect agrees to make any amendment(s) to PHI in a Designated Record Set that County directs or agrees to pursuant to 45 CFR § 164.526 at the request of County or an Individual, within thirty (30) calendar days of receipt of said request by County. Riskconnect agrees to notify County in writing no later than ten (10) calendar days after said amendment is completed.
- I. Riskconnect 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 Riskconnect on behalf of, County available to County and the Secretary in a time and manner as determined by County or as designated by the Secretary for purposes of the Secretary determining County's compliance with the HIPAA Privacy Rule.
- J. Riskconnect agrees to document any Disclosures of PHI County discloses to Riskconnect or Riskconnect creates, receives, maintains, or transmits on behalf of County, and to make information related to such Disclosures available as would be required for County to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 CFR § 164.528.
- K. Riskconnect agrees to provide County or an Individual, as directed by County, in a time and manner to be determined by County, that information collected in accordance with this Contract, in order to permit County to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 CFR § 164.528.
- L. Riskconnect agrees that to the extent Riskconnect carries out County's obligation under the HIPAA Privacy and/or Security rules Riskconnect will comply with the requirements of 45 CFR Part 164 that apply to County in the of such obligation.
- M. Riskconnect shall work with County upon notification by Riskconnect to County of a Breach to properly determine if any Breach exclusions exist as defined in Section 2.2(b)(i).

## 2.4 Security Rule

- A. Riskconnect 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, and § 164.316 with respect to electronic PHI County discloses to Riskconnect or Riskconnect creates, receives, maintains, or transmits on behalf of County. Riskconnect shall follow generally accepted system security principles and the requirements of the HIPAA Security Rule pertaining to the security of electronic PHI.
- B. Riskconnect shall ensure that any subcontractors that create, receive, maintain, or transmit electronic PHI on behalf of Riskconnect agree through a contract with Riskconnect to the same restrictions and requirements contained in this Section 2.4.
- C. Riskconnect shall report to County immediately any Security Incident of which it becomes aware. Riskconnect shall report Breaches of Unsecured PHI in accordance with Section 2.5 and as required by 45 CFR § 164.410.

## 2.5 Breach Discovery and Notification

- A. Following the discovery of a Breach of Unsecured PHI, Riskconnect shall notify County of such Breach, however both parties agree to a delay in the notification if so, advised by a law enforcement official pursuant to 45 CFR § 164.412.
  - i. A Breach shall be treated as discovered by Riskconnect as of the first day on which such Breach is known to Riskconnect or, by exercising reasonable diligence, would have been known to Riskconnect.
  - ii. Riskconnect shall be deemed to have knowledge of a Breach, if the Breach is known, or by exercising reasonable diligence would have known, to any person who is an employee, officer, or other agent of Riskconnect, as determined by federal common law of agency.
- B. Riskconnect shall provide the notification of the Breach immediately to the County Privacy Officer at 714.834.3154. Riskconnect's notification may be oral but shall be followed by written notification within 24 hours of the oral notification.

- C. Riskconnect's notification shall include, to the extent possible:
- i. The identification of each Individual whose Unsecured PHI has been, or is reasonably believed by Riskconnect to have been, accessed, acquired, used, or disclosed during the Breach.
  - ii. Any other information that County is required to include in the notification to Individual under 45 CFR §164.404 (c) at the time Riskconnect is required to notify County 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 Riskconnect 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.
- D. County may require Riskconnect to provide notice to the Individual as required in 45 CFR § 164.404, if it is reasonable to do so under the circumstances, at the sole discretion of the County.
- E. In the event that Riskconnect is responsible for a Breach of Unsecured PHI in violation of the HIPAA Privacy Rule, Riskconnect shall have the burden of demonstrating that Riskconnect made all notifications to County consistent with this Section 2.5 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.
- F. Riskconnect 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.
- G. Riskconnect shall provide to County all specific and pertinent information about the Breach, including the information listed in Section 2.5(c)(ii)(A)-(E), if not yet provided, to permit County 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 Riskconnect's initial report of the Breach to County pursuant to Section 2.5(b).
- H. Riskconnect shall continue to provide all additional pertinent information about the Breach to County as it may become available, in reporting increments of five (5) business days after the last report to County. Riskconnect shall also respond in good faith to any reasonable requests for further information, or follow-up information after report to County, when such request is made by County.
- I. Subject to any applicable limitations in the Contract, Riskconnect shall bear all expense or other costs associated with the Breach and shall reimburse County for all expenses County incurs in addressing the Breach and consequences thereof, including costs of investigation, notification, remediation, documentation or other costs associated with addressing the Breach.

## 2.6 Permitted Uses and Disclosures by Riskconnect

- A. Riskconnect may use or further disclose PHI County discloses to Riskconnect as necessary to perform functions, activities, or services for, or on behalf of, County as specified in this Contract, provided that such use or Disclosure would not violate the HIPAA Privacy Rule if done by County except for the specific Uses and Disclosures set forth below.
- i. Riskconnect may use PHI County discloses to Riskconnect, if necessary, for the proper management and administration of Riskconnect.
  - ii. Riskconnect may disclose PHI County discloses to Riskconnect for the proper management and

administration of Riskconnect or to carry out the legal responsibilities of Riskconnect, if:

- a. The Disclosure is required by law; or
  - b. Riskconnect obtains reasonable assurances from the person to whom 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 and the person immediately notifies Riskconnect of any instance of which it is aware in which the confidentiality of the information has been breached.
  - iii. Riskconnect may use or further disclose PHI County discloses to Riskconnect to provide Data Aggregation services relating to the Health Care Operations of Riskconnect.
- B. Riskconnect may use PHI County discloses to Riskconnect, if necessary, to carry out legal responsibilities of Riskconnect.
  - C. Riskconnect may use and disclose PHI County discloses to Riskconnect consistent with the minimum necessary policies and procedures of County.
  - D. Riskconnect may use or disclose PHI County discloses to Riskconnect as required by law.

## 2.7 Obligations of County

- A. County shall notify Riskconnect of any limitation(s) in County's notice of privacy practices in accordance with 45 CFR § 164.520, to the extent that such limitation may affect Riskconnect's Use or Disclosure of PHI.
- B. County shall notify Riskconnect 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 Riskconnect's Use or Disclosure of PHI
- C. County shall notify Riskconnect of any restriction to the Use or Disclosure of PHI that County has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Riskconnect's Use or Disclosure of PHI.
- D. County shall not request Riskconnect to use or disclose PHI in any manner that would not be permissible under the HIPAA Privacy Rule if done by County.

## 2.8 Business Associate Termination

- A. Upon County's knowledge of a material breach or violation by Riskconnect of the requirements of this Section 20.3, County shall:
  - i. Provide an opportunity for Riskconnect to cure the material breach or end the violation within thirty (30) business days; or
  - ii. Immediately terminate this Contract, if Riskconnect is unwilling or unable to cure the material breach or end the violation within (30) days, provided termination of this Contract is feasible.
- B. Upon termination of this Contract, Riskconnect shall either destroy or return to County all PHI Riskconnect received from County or Riskconnect created, maintained, or received on behalf of County in conformity with the HIPAA Privacy Rule.
  - i. This provision shall apply to all PHI that is in the possession of subcontractors or agents of Riskconnect.
  - ii. Riskconnect shall retain no copies of the PHI.
  - iii. In the event that Riskconnect determines that returning or destroying the PHI is not feasible, Riskconnect shall provide to County notification of the conditions that make return or destruction infeasible. Upon determination by County that return or destruction of PHI is infeasible, Riskconnect shall extend the protections of this Business Associate Contract to such PHI and limit further Uses and Disclosures of such PHI to those purposes that make the return or destruction infeasible, for as long as Riskconnect maintains such PHI.
- C. The obligations of this Attachment H shall survive the termination of this Contract.

## ATTACHMENT E RISKONNECT PRIVACY STATEMENT

Riskconnect respects County's privacy and is committed to protecting County's personal data. This privacy policy will inform County as to how Riskconnect looks after County's personal data and tell County about County's privacy rights and how the law protects County.

Please also use the Glossary to understand the meaning of some of the terms used in this privacy policy.

### 1. Important information and who we are

#### Purpose of this privacy policy

This privacy policy sets out the basis on which any personal data collected from you, or that you provide, will be processed by Riskconnect as a controller. It does not relate to our processing activities we carry out as a processor on behalf of our clients. Requests and queries relating to processing we conduct as processor should be directed to the relevant controller of your personal data.

We do not knowingly collect data relating to children.

It is important that you read this privacy policy together with any other privacy policy or fair processing policy we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data. This privacy policy supplements other notices and privacy policies and is not intended to override them.

#### Controller

We may share your personal data with any member of our group, which means our affiliates and subsidiaries (the "Riskconnect Group"). This privacy policy is issued on behalf of the Riskconnect Group so when we mention "Riskconnect", "we", "us" or "our" in this privacy policy, we are referring to the relevant company in the Riskconnect Group responsible for processing your data. We will let you know which entity will be the controller for your data when you purchase a product or service with us.

Riskconnect Inc. is the controller and responsible for this website.

We have appointed a Data Privacy Committee ("DPC") who is responsible for overseeing questions in relation to this privacy policy. If you have any questions about this privacy policy, including any requests to exercise your legal rights, please contact the DPC using the details set out below.

#### Contact details

If you have any questions about this privacy policy or our privacy practices, please contact our DPC in the following ways:

##### Full name of legal entity:

Riskconnect Inc.

##### Email Address:

dpc@riskconnect.com

##### Postal Address:

Data Privacy Committee (DPC)  
1701 Barrett Lakes Blvd, NW, Suite 500  
Kennesaw, GA 30144  
USA

We are committed to working with you to obtain a fair resolution of any complaint or concern about privacy. If, however, you believe that we have not been able to assist with your complaint or concern, and you are located in the EEA, you have the right to lodge a complaint with the competent supervisory authority.

#### Changes to the privacy policy and your duty to inform us of changes

We keep our privacy policy under regular review. Any additions or modifications will be included in an updated privacy policy posted on our website. This version was last updated on December 2020.



It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

### Third-party links

This website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy policy of every website you visit.

## 2. The data we collect about you and how we use it

Personal data means any information about an individual from which that person can be identified. It does not include data where the identity has been removed and cannot be ascertained from that information alone or in conjunction with other information (anonymous data).

You may provide personal data to us when you interact with us on behalf of your organization. We may collect, use, store and transfer different kinds of personal data about you and we will only use your personal data when the law allows us to. We have set out below, in a table format, a description of the data we collect, how we plan to use your personal data, and, for the purposes of data relating to individuals based in the EU or the UK, which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Your **Identity and Contact Data** such as your name, email address, office and cell phone number and LinkedIn URL.

Purpose	Legal basis
To register your organization as a new customer	Performance of a contract with you
To manage our relationship with you which will include: (a) answer queries and respond to your requests that you make to us; (b) notify you of changes to our terms or privacy policy; (c) handle user support requests	Necessary for our legitimate interests (to run our business, manage our relationship with you and keep our records updated) Performance of a contract with you Necessary to comply with a legal obligation
To manage event registration	Performance of a contract with you Necessary for our legitimate interests (to run our business and manage our relationship with you)
To provide our services to you	Performance of a contract with you
To send you information about our products and services.	Necessary for our legitimate interests (to keep you updated of products and services, to run our business)

Purpose	Legal basis
To register your organization as a new customer	Performance of a contract with you
To provide relevant content and products and services to you	Performance of a contract with you Necessary for our legitimate interests (to run our business, manage our relationship with you)

Your **Professional and Employment Data** such as the name of your employer, job title, work history and experience in presenter bios collected for events, presentations, marketing collateral, and testimonials in connection with our business activities.

Your **Financial and Transaction Data** such as purchase history, financial details and payment information.

Purpose	Legal basis
To take payment and give refunds.	Performance of a contract with you
To keep a record of any financial transactions with you	Performance of a contract with you Necessary for our legitimate interests (to run our business, manage our relationship with you and keep our records updated).

Your **Technical Data** about your device. This includes things like your IP address and approximate location information, login data, browser type and version, browser connection string, system settings, browsing actions and patterns, operating system and platform, and other technology on the devices you use to access our website.

Purpose	Legal basis
To administer and protect our business and this website.	Necessary for our legitimate interest (for running our business, provision of IT and administration services, network security, growing our business and informing our marketing strategy). Necessary to comply with a legal obligation.
To deliver relevant website content to you.	Necessary for our legitimate interests (to define types of customers, to keep our website updated and relevant, to develop our business and to inform our marketing strategy).
To improve our website and services.	Necessary for our legitimate interests (to keep our website updated and relevant, to develop our business and services).

Your **Usage Data** about how you use our website as well as your preferences regarding products and services.

Purpose	Legal basis
To make suggestions and recommendations to you about goods or services that may be of interest to you.	Necessary for our legitimate interest (to develop and grow our business, to develop our products/services and inform our marketing strategy).

Your **Marketing and Communications Data** such as your preferences in receiving marketing from us and our third parties and your communication preferences.

Purpose	Legal basis
To deliver relevant marketing content to you and measure or understand the effectiveness or the marketing we serve to you.	Necessary for our legitimate interests (to study how customers use our services, to grow our business and to inform our marketing strategy)

We also collect, use and share Aggregated Data such as statistical or demographic data for any purpose. Aggregated Data could be derived from your personal data but is not considered personal data in law as this data will **not** directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific website feature. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this privacy policy.

We do not collect any Special Categories of Personal Data about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health, and genetic and biometric data). Nor do we collect any information about criminal convictions and offences.

**If you fail to provide personal data**

Where we need to collect personal data by law, or under the terms of a contract we have with you, and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with services). In this case, we may have to cancel a service you have with us but we will notify you if this is the case at the time.

**Consent**

Generally, we do not rely on consent as a legal basis for processing your personal data although we will get your consent before sending third party direct marketing communications to you via email or text message. You have the right to withdraw consent to marketing at any time by contacting us.

**Marketing**

We strive to provide you with choices regarding certain personal data uses, particularly around marketing and advertising.

We may use your personal data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which services may be relevant for you (we call this marketing).

You will receive marketing communications from us if you have requested information from us, purchased services from us or where we think our services will be of interest to you and you have not opted out of receiving that marketing.

**Opting out**

You can ask us to stop sending you marketing messages at any time by following the opt-out links on any marketing message sent to you or by contacting us at any time at [dpc@riskconnect.com](mailto:dpc@riskconnect.com).

Where you opt out of receiving these marketing messages, we may still send you non-marketing related messages in relation to a purchase, service experience or other transaction that you have made.

**Cookies**

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of this website may become inaccessible or not function properly.

**Change of purpose**

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us.

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

**3.How is your personal data collected?**

We use different methods to collect data from and about you including through:

**Direct interactions.** You may give us your personal information by filling in forms or by corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you:

- register to use our website
- request information regarding our services
- purchase or sell products or services on behalf of your organization
- request marketing to be sent to you
- request customer support
- sign up to an event such as a webinar or conference; or

- give us feedback or contact us.

**Automated technologies or interactions.** As you interact with our website, we will automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies and other similar technologies.

**Third parties or publicly available sources.** We may also receive personal data about you from various third parties from whom we purchase personal data or collect from publicly available information. The personal data we collect from other sources includes identifiers, professional or employment-related information, education information, visual information, internet activity information, and inferences about preferences and behaviors. In particular, we collect personal data from the following sources:

- Third party providers of business contact information, including mailing addresses, job titles, email addresses, phone numbers, intent data (or user behavior data), IP addresses, social media profiles, LinkedIn URLs and custom profiles, for purposes of targeted advertising, delivering relevant email content, event promotion and profiling, determining eligibility, and verifying contact information; and
- Other individuals at your organization who may provide us with your contact details for the purposes of obtaining services.

#### **4. Disclosures of your personal data**

We may share your personal data with various third parties as follows:

##### **Service Providers:**

We will share your personal data with our contracted service providers who provide services such as IT and system administration and hosting, credit card processing, research and analytics, marketing, customer support, and data enrichment for the purposes and pursuant to the legal bases described above; such service providers comprise companies located in countries including USA, UK, Singapore, Australia, India, Germany, and Ireland.

##### **Event Sponsors:**

If you attend an event, conference, or webinar organized by us, or download or access an asset on our website, we may share your personal data with sponsors of the event. If required by applicable law, you may consent to such sharing via the registration form or by allowing your attendee badge to be scanned at a sponsor booth. In these circumstances, your information will be subject to the sponsors' privacy statements. If you do not wish for your information to be shared, you may choose to not opt-in via event/webinar registration or elect to not have your badge scanned.

##### **Customers with whom you are affiliated:**

If you use our services as an authorized user of one of our customers, we may share your personal data with our customer responsible for your access to the services to the extent this is necessary for verifying accounts and activity, investigating suspicious activity, or enforcing our terms and policies.

##### **Third party networks and websites:**

With third-party social media networks, advertising networks and websites, so that we can market and advertise on third party platforms and websites.

##### **Professional Advisers:**

In individual instances, we may share your personal data with professional advisers acting as service providers, processors, or joint controllers – including lawyers, bankers, auditors, and insurers based in countries in which we operate who provide consultancy, banking, legal, insurance and accounting services, and to the extent we are legally obliged to share or have a legitimate interest in sharing your personal data.

##### **Riskconnect Affiliates:**

We share your personal data with the Riskconnect Group and companies that we acquire in the future after they are made part of the Riskconnect Group, to the extent such sharing of data is necessary to fulfil a request you have

submitted via our websites or for customer support, marketing, technical operations, and account management purposes. Riskconnect affiliated companies are currently located in the United States, UK, and India.

We may also share personal data with third parties to whom we may choose to sell, transfer or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this privacy policy.

We require all third parties to respect the security of your personal data and to treat it in accordance with the law.

### **5. International transfers**

Your personal data may be collected, accessed, transferred to, and stored by us in the United States and by our affiliates and third parties disclosed above in section 4 that are based in other countries.

Whenever we transfer your personal data to these third parties, we ensure that the recipient of your personal data offers an adequate level of protection and security, for instance by entering into Standard Contractual Clauses or any other alternative mechanism for the transfer as approved by the European Commission under Article 46 of the General Data Protection Regulation or other applicable regulator.

Please contact us if you want further information on the specific mechanism used by us when transferring data to third parties.

### **6. Data security**

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions, and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

### **7. Data retention**

How long will you use my personal data for?

We will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

For individuals based in the EU or UK, in some circumstances you can ask us to delete your data see your legal rights in the EU and the UK below for further information.

In some circumstances we will anonymize your personal data (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

### **8. Your legal rights in the EU and the UK**

RESERVED

### **9. California Privacy Rights**

California residents have the right to receive information that identifies any third parties with whom we have shared your personal data for that third party's own marketing purposes within the previous calendar year, as well as a description of the categories of Personal Information disclosed to that third party. You may obtain this information once a year and free of charge by contacting the Data Privacy Committee at [dpc@riskconnect.com](mailto:dpc@riskconnect.com).

Your 'Do Not Track' Browser Setting. Some web browsers incorporate a Do Not Track ("DNT") feature that signals to the websites that you visit that you do not want to have your online activity tracked. At this time, our website does not respond to DNT signals. Other third-party websites may keep track of your browsing activities when they provide you with content, which enables them to customize what they present to you on their websites.



## 10. Glossary

### LAWFUL BASIS

Legitimate Interest means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us.

Performance of a Contract means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.

Comply with a legal obligation means processing your personal data where it is necessary for compliance with a legal obligation that we are subject to.

**ATTACHMENT F**  
**SUPPLEMENTAL TERMS AND CONDITIONS (RISKONNECT APPLICATIONS)**

Solely to the extent required by Riskconnect's contract with salesforce.com that is applicable to this Contract

**SUPPLEMENTAL TERMS AND CONDITIONS (RISKONNECT APPLICATIONS)**

The following Additional and Amended Definitions, Additional Terms and Conditions and Additional Exhibits are incorporated into the Agreement by reference

All defined terms in this Appendix A have the meanings set forth in the General Terms and Conditions, as and to the extent amended below.

1. *Additional and Amended Definitions*

- 1.1 *"Data Infrastructure" means the data processing resources within the Riskconnect Service, including but not limited to, data and file storage, within County's account configured in the Riskconnect Service platform.*
- 1.2 *"Licensors" shall also include:*
- 1.2.1 *salesforce.com (Platform Provider);*
- 1.2.2 *Rackspace (secure server environment for converting source data);*
- 1.2.3 *Adobe EchoSign (e-signature); and*
- 1.2.4 *Domo (Riskconnect Insights data visualization).*
- 1.3 *"Platform Provider" means Salesforce.com, Inc.*
- 1.4 *"Platform Service" means the online, web-based service provided by Platform Provider to Riskconnect in connection with Riskconnect's provision of the Riskconnect Service.*
- 1.5 *"System Administrator" means a User designated by County who is authorized to create User accounts, to purchase subscriptions by executing a Subscription Order, and to otherwise administer County's use of the Riskconnect Service.*

2. *Additional Terms and Conditions*

- 2.1 *Sole Provider. Notwithstanding any access County's Users may have to the services of Riskconnect's Licensors via the County's configuration of the Riskconnect Service, Riskconnect is the sole provider of the Riskconnect Service and County is entering into a contractual relationship solely with Riskconnect. In the event that Riskconnect ceases operations or otherwise ceases or fails to provide the Riskconnect Service, Riskconnect's Licensors have no obligation to refund County any fees paid by County to Riskconnect or to provide County the Riskconnect Service.*
- 2.2 *Modifications Performed by County. Any configuration, development, or data integration services to the County's instance of the Riskconnect Service that is performed by County or County's third parties is not covered by Software Support and Riskconnect shall have no liability whatsoever for such services. However, County may request Riskconnect to render support services for configurations and modifications performed by County provided that such Annual Services shall be billable to County at Riskconnect's then current hourly rate.*
- 2.3 *Data Infrastructure. County's subscription includes a specific quantity of Data Infrastructure, as set forth on the applicable Subscription Order. The Riskconnect Service includes administrative features that permit County's System Administrator(s) to view and monitor County's utilization of Data Infrastructure. If County exceeds the amount of Data Infrastructure as set forth in the Subscription Order, County shall be charged for any additional Data Infrastructure used and pay additional subscription fees. Provided that any such changes do not adversely impact County Data Infrastructure limits or rights as agreed to in this Contract, Riskconnect reserves the right to establish or modify with thirty (30) days' notice its general Data Infrastructure practices and limits, provided the minimum amount of storage included without additional charge may not be modified without County's prior written consent.*
- 2.4 *RESERVED.*

- 2.5 *Licensors' Warranty Disclaimer. NOTHING IN THIS Appendix A, SECTION Error! Reference source not found. SHALL LIMIT RISKONNECT'S WARRANTIES OR INDEMNIFICATION OBLIGATIONS UNDER THIS AGREEMENT, INCLUDING THOSE THAT RISKONNECT MAKES AND/OR PROVIDES ON BEHALF OF RISKONNECT'S LICENSORS. Notwithstanding the foregoing, , to the maximum extent permitted by law, Riskonnect's Licensors make no, and disclaim all, warranties of any kind, whether express, implied, statutory, or otherwise, including, without limitation, any implied warranty of merchantability, fitness for a particular purpose, or non-infringement of third-party rights with respect to the Platform Service, and/or the Riskonnect Service, or any of the products and services offered by Riskonnect's Licensors. Riskonnect's Licensors make no representation, warranty, or guaranty as to the reliability, timeliness, quality, suitability, availability, accuracy or completeness of the Riskonnect Service. Riskonnect's Licensors do not represent or warrant that the Riskonnect Service will be available, secure, timely, uninterrupted or error-free; the Riskonnect Service or any of the products and services offered by Riskonnect's Licensors will meet County's requirements or expectations; any data stored using the Riskonnect Service will be accurate, reliable, or secure; errors or defects in the Riskonnect Service will be corrected; or the Riskonnect Service or the Data Infrastructure used by Riskonnect to make the Riskonnect Service available are free of Disabling Code, viruses or other harmful components.*
- 2.6 *Third-Party Beneficiaries. There are no third-party beneficiaries to this Agreement, except Platform Provider shall be a third-party beneficiary to this Agreement solely as it relates to the provisions herein that relate to the use of the Platform Service.*
- 2.7 *Data Portability and Deletion.*
- 2.7.1 *After Termination or Expiration. In the event this Agreement terminates for any reason, within 30 days after the effective date of termination, Riskonnect shall make available to County a file of County Data in CSV file format and in the Riskonnect Service layout; and Riskonnect may thereafter delete County Data.*

*The transfer of County Data shall be governed by the Data Transfer Protocols at <https://riskonnect.com/legal-dtps/>.*

---

## ATTACHMENT G COUNTY'S USER PROVISIONING POLICY

### OC-SEC-POL-003 – User Provisioning Policy

<b>Policy Owner:</b>	CISO	<b>Effective Date:</b>	12/09/2021
<b>Prepared By:</b>	CEO/IT	<b>Version No.:</b>	1.0
<b>Approved By:</b>	CEO	<b>Publication Date:</b>	PENDING
<b>Approval Date:</b>	PENDING	<b>Next Review:</b>	TBD

#### 1 Policy Statement

All County resource owners must safeguard County assets by ensuring that only authorized workforce members are granted access rights and that changes to those access rights are communicated in a proper and timely manner and acted upon in a uniform and auditable way.

- **Purpose**

Issues of access and security are everyone's responsibility and are not isolated to a single agency, department, location, login credential, or system. This document establishes countywide user provisioning policy ("Policy") and is intended to mitigate risks associated with access to County assets granted to workforce members by establishing parameters for the provisioning and deprovisioning of that access.

- **Applicability**

This Policy applies to all County workforce members (employees, consultants, temporary help, contractors, vendors and volunteers) with access to County assets. *Access* encompasses the mechanisms for logical (e.g., user IDs, passwords, etc.) as well as physical (e.g., keys, badges, etc.) access.

- **Responsibility**

It is the responsibility of agency/department heads and those designated by him or her, including supervisors and IT and Human Resources staff, to ensure compliance with this Policy.

- **Policy Description**

Changes in workforce member access to County resources must be reviewed, documented, communicated and executed in a timely manner to prevent unauthorized access to County assets.

- **User Access:** Only authorized users are allowed access to County assets. Access is granted to assets/systems based on the principle of least privilege, which limits access to that which is necessary for the specific user to perform his/her job. In granting access, consideration must be given to the user's role/job function. Access should not just be granted based solely upon the privileges of the user's predecessor. Access requests are to be approved by the user's department head or designee and/or the relevant system owner before access is granted. Prior to being granted access to information assets, each user must complete the County's Workforce Member Usage Agreement.
- **User Credentials:** Each workforce member must have their own unique ID that is not reused, shared or subsequently reassigned. User IDs, passwords and authentication and security methods must comply with applicable regulatory standards and County policies.
- **Timeline for Compliance:** Within 24 hours of a workforce member's change in status, County asset owners must be notified of the change. Within 48 hours of a change in status, required access changes must be completed and auditable. Any time a workforce member's need to access County assets is terminated, suspended or changed, for any reason, the member's agency/department must take immediate action to prevent possible or actual unauthorized access to County assets.

- **Change in Status Due to Disciplinary Action:** Workforce members who are involuntarily terminated, put on administrative leave and/or subjected to other disciplinary action (e.g., suspension) requiring a change in access to County assets shall have their access disabled or terminated immediately.
- **Changes Other Than Disciplinary Action:** Changes resulting in prolonged periods of workforce member inactivity (e.g., leave of absence, temporary reassignment) and changes resulting in different work requirements (e.g., transfers to another division or department) shall be considered a change of status under this Policy.
- **Special Conditions:** Any special conditions related to a person's change in status (e.g., continuing confidentiality rights, revocation of access to information to which the workforce member may have had access previously) will be reviewed with the affected workforce member during the member's "out-processing".
- **Development of Adequate Procedures:** Each agency/department must adopt procedures sufficient to ensure that the agency/department is able to meet the conditions set forth in this Policy. This includes development of a methodology to account for and determine each workforce member's access levels in order to facilitate complete de-provisioning when required; periodic confirmation/review of active user access levels; routine maintenance to remove disabled and inactive accounts; and utilization of employee separation checklists to ensure consistency in de-provisioning.

- **DEFINITIONS**

Term	Definition
Change in Status	Any change in assigned agency, department, access role, or system asset to which the workforce member has access.
County Asset	Any information, credential, physical location and/or device that the County owns, manages or regulates.
County Asset Owner	The agency/department and personnel designated to assign, track, maintain and terminate workforce member access to a County asset.
Involuntary Termination	The removal of an employee under involuntary or adverse conditions, including termination, involuntary transfer, or any other situation that could result in a loss of County information assets.
Workforce Member	Members of the County workforce including employees, temporary help, contractors, vendors and volunteers.

- **Related Documents**

No	Title	Issued By
OC-SEC-POL-001	Information Technology (IT) Usage Policy	CEO
OC-SEC-POL-002	Countywide Security Policy	CEO
Agy -SEC-PRO-003	Agency User Provisioning Procedure	Agency

- **Revision History**

Date	By	Ver #	Description
07/13/11	TBD	1.0	First published version.

- **Approvals**

Date	Approver Names	Signature
01/28/11	Countywide Provisioning Work Group	See meeting minutes
02/09/11	Technology Council	See meeting minutes
07/21/11	Executive Council	See meeting minutes



## ATTACHMENT H

### DATA CLASSIFICATION POLICY

Policy Area	IT Policy Library
Approved Date	TBD
Approved By	CISO
Effective Date	December 10, 2021
Current Version	1.0

#### 1. OVERVIEW

Data Classification provides a framework for managing data assets based on value and associated risks and for applying the appropriate levels of protection as required by state and federal law as well as proprietary, ethical, operational, and privacy considerations. All County of Orange data, whether electronic or printed, should be classified. The data owner, who is responsible for selecting the Data Classification, should consult with legal counsel on the classification of data as Public, Confidential, Regulated, and Sensitive. Consistent use of data classification reinforces with users the expected level of protection of County of Orange data assets in accordance with County of Orange security policies.

#### 2. PURPOSE

The purpose of this policy is to provide a foundation for the development and implementation of necessary security controls to protect information according to its value and/or risk. Security standards, which define these security controls and requirements, may include: document marking/labeling, release procedures, privacy, transmission requirements, printing protection, computer display protections, storage requirements, destruction methods, physical security requirements, access controls, backup requirements, transport procedures, encryption requirements, and incident reporting procedures.

#### 3. SCOPE

This policy applies to all Staff that uses County of Orange Information Resources.

#### 4. POLICY

Data shall be classified as listed below.

- 4.1 Public: - Information intended or required for public release. Information can only be declared Public by an authorized Data Owner which would include the Board of Supervisors, Elected officials, and their designees such as Public Information Officers (PIO) or representative legal counsel. Disclosure of such information should not adversely impact County of Orange's business operations, financial well-being, or our image and reputation.
- 4.2 Confidential – Information which relates to the internal work products of the County. This is the default classification whenever a classification has not been assigned. Confidential data may be subject to disclosure or release under an approved California Public Records (PRA) request, however such disclosure does not change the data classification of that data. Examples of Confidential data may include but are not limited to:
  - Operational information
  - General memos, emails, and correspondence
  - Personnel records (not protected by regulation)
  - General Research
- 4.3 Regulated – this information must be protected from unauthorized disclosure or public release based on state or federal law, and other constitutional, statutory, judicial, and legal agreements. This type of information requires additional levels of control and protection. Examples of "Regulated" information may include but are not limited to:

- Personally Identifiable Information, such as: a name in combination with Social Security Number (SSN) and/or financial account numbers
  - Intellectual Property, such as: Copyrights, Patents and Trade Secrets
  - Medical Records
- 4.4 Secure –Highly sensitive data is such that if disclosed such information could harm the County of Orange’s business operations. This type of Data is protected under exemptions within the California Public Records Act (PRA). Access is restricted to named authorized personnel and is protected by specialized access controls, and encryption, or both. Examples of sensitive data may include but are not limited to:
- Network Drawings
  - Infrastructure system credentials
  - Information security procedures

Note: Access to all but Public data shall be authenticated and logged.

## 5. ENFORCEMENT

Any workforce member found to have violated this policy may be subject to disciplinary action, up to and including termination.

## 6. DISTRIBUTION

This policy is to be distributed to all County of Orange Staff and information Technology contractors.

## 7. Policy History

Version	Date	Description	Approved By
1.0	1/1/2013	Initial policy release	TBD