



CONTRACT # MA-017-14010752

BETWEEN

THE COUNTY OF ORANGE/RISK MANAGEMENT

AND

RISKONNECT INC.

FOR

RISK AND CLAIMS MANAGEMENT INFORMATION

SYSTEM SOLUTION

CONTRACT # MA-017-14010752

FOR

RISK AND CLAIMS MANAGEMENT INFORMATION SYSTEM SOLUTION

This Agreement, (hereinafter referred to as "Contract"), to provide Risk and Claims Management Information System, effective December __, 2013 (the "Effective Date") by and between Riskconnect, Inc. with a place of business at Barrett Lakes Blvd, Suite 500, Kennesaw GA 30144, (hereinafter referred to as "Riskconnect"), and the County of Orange, a political subdivision of the State of California, (hereinafter referred to as "County") which may be referred to individually as "Party" or collectively as "Parties".

RECITALS

WHEREAS, Riskconnect responded to a Request for Proposal (RFP) to provide a Risk and Claims Management Information System Solution and Services; and

WHEREAS, Riskconnect represented that its proposed services meet or exceed the requirements and specifications of the RFP; 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;

NOW, THEREFORE, the Parties mutually agree as follows:

ARTICLES

1. **Term of Contract:** The Term ("Term") of this Contract shall be for Five (5) years from the Effective Date and may be extended 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 the Riskconnect in writing with at least a sixty (60) day notice before the end of the Term.
2. **Scope of Work:** The Scope of Work for this Contract is attached hereto as Attachments A, D, E, F, G and H. The services to be provided by Riskconnect thereunder are referred herein as the "Services."
3. **Compensation:** Riskconnect agrees to accept the specified compensation as set forth in Attachment B, Cost/Compensation, 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 the Riskconnect of all its duties and obligations hereunder.
4. **Entire Contract:** This Contract, comprised of these terms and conditions, Attachments A, B, C, D, E, F, G, H, I, J, K, and L, which are incorporated herein, 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.
5. **Amendments:** No alteration or variation of the terms of this Contract shall be valid unless made in writing and signed by the Parties.
6. **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.

7. **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.
8. **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 testing set forth in accordance with Section 47 herein.
9. **Warranty:** Riskonnect 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 was originally provided to You 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.

The only warranty offered by Salesforce.com [Riskonnect's platform licensor] to the County in connection with this Contract is expressly provided in Attachment J (Platform Continuity Warranty) attached hereto and incorporated herein.

Except as provided above, Riskonnect's licensors make no warranties of any kind, including but not limited to with respect to the service, and/or the Riskonnect application, whether express, implied, statutory or otherwise. Riskonnect's licensors make no representation, warranty, or guaranty as to the reliability, timeliness, quality, suitability, availability, accuracy or completeness of Riskonnect's application. Riskonnect's licensors do not represent or warrant that (a) the Riskonnect application will be available, secure, timely, uninterrupted or error-free, or any other application, software, hardware, system or data, (b) the Riskonnect system or the service will meet your requirements or expectations, (c) any data stored using the Riskonnect application will be accurate, reliable, or secure, (d) errors or defects in Riskonnect's application or the service will be corrected, or (e) the Riskonnect application or the systems used by Riskonnect to make the Riskonnect application available are free of viruses or other harmful components. To the maximum extent permitted by law, Riskonnect's licensors disclaim all conditions, representations and warranties, whether express, implied, statutory or otherwise, with respect to Riskonnect's application and the service, including, without limitation, any implied warranty of merchantability, fitness for a particular purpose, or non-infringement of third party rights.

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.

10. **Patent/Copyright Materials/Proprietary Infringement:** Unless otherwise expressly provided in this Contract, Riskonnect shall be solely responsible for clearing the right to use any patented or copyrighted materials in the performance of this Contract. Riskonnect 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. Riskonnect agrees that, in accordance with the more specific requirement contained in Section 17 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.
11. **Compliance with Laws:** Riskonnect represents and warrants that Services to be provided under this Contract shall fully comply, at Riskonnect'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. Riskonnect acknowledges that County is relying on Riskonnect to ensure such compliance, and pursuant to the requirements of Section 17 below, Riskonnect 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.
12. **Performance:** Riskonnect shall perform all Services under this Contract, taking necessary steps and precautions to perform the Services to in accordance with Section 2 above. Riskonnect shall be responsible for the professional quality, technical assurance, timely completion and coordination of all documentation and other /services furnished by Riskonnect under this Contract. Riskonnect 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.

- 13. 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 47.
- 14. Conditions Affecting Work:** The 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 the 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.
- 15. Insurance Provisions:** 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 self-insured retention (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 to the County for the full term of this Contract, the County may terminate this Contract in accordance with Section 19 ("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 be 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:

<u>Coverage</u>	<u>Minimum Limits</u>
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)	\$10,000,000 per claim/ in the aggregate

Liability)

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.

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 on the solicitation.

If Riskconnect fails to provide the insurance certificates and endorsements within ten days of notification by CEO/Purchasing or the agency/department purchasing division, award may be made to the next qualified Riskconnect.

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.

16. **Limitation of Liability.** Neither Party to this Contract be liable for injury or damage to business, lost profits, revenues or goodwill of any party hereto, or for any special, consequential, or incidental damages, whether for breach of warranty, breach of contract, repudiation of contract, termination, negligence, or otherwise, even if it shall have been advised of the possibility of such damages, excepting, however, any damages or other cost, expense or liability arising from an indemnification obligation, breach of confidentiality, death, personal injury, property damage, gross negligence, or willful misconduct.

In no event shall either Party's aggregate liability exceed the amounts actually paid by the County 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 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.

IN NO EVENT SHALL RISKONNECT'S LICENSORS HAVE ANY LIABILITY TO THE 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 YOU HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Indemnification:

Subject to the limitation set forth herein, Riskonnect 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 Riskonnect of this Contract; or (ii) a claim alleging Riskonnect'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 Riskonnect; (b) give Riskonnect sole control of the defense and settlement of the claim (provided that Riskonnect (1) shall provide to the County written confirmation that Riskonnect acknowledges Riskonnect's obligations to indemnify the County for such claim; (2) shall provide to the County evidence of Riskonnect's ability to defend and settle such claim, to the reasonable satisfaction of the County; and (3) may not settle any claim unless Riskonnect and the third party(ies) unconditionally release the County of all liability and such settlement does not affect the County's business or the Riskonnect Service); (c) provides to Riskonnect all available information and assistance at Riskonnect's sole cost and expense; and (d) has not compromised or settled such claim.

For clarity, Riskonnect 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 Riskonnect.

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

18. 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 Riskonnect to stop and proceed no further until such time as Riskonnect 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. Riskonnect 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.

19. Breach: The failure of Riskonnect 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 Riskonnect 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 Riskonnect for and during the period in which the Riskonnect 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.

20. Disputes: The 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.

21. Termination by the County for Convenience: The County shall have the right to terminate for its convenience, at any time and for any reason or no reason: (a) the Term of this Contract with regard to the Services, or (b) any portion of the Services, then being provided by Riskconnect. Any such termination shall be effected by the County sending to Riskconnect a written notice of termination specifying the extent of the Services being terminated and the intended date (the "Termination Date") upon which, at 11:59 p.m., such termination shall be effective (any such notice, a "Termination Notice"). The Termination Date specified in any such Termination Notice sent by the County pursuant to this Section shall be at least ninety (90) days after the date of such Termination Notice, with the understanding that subscription fees paid by Riskconnect to Riskconnect's platform licensor are for annual periods, paid in advance and are non-cancellable and non-refundable during each annual contract period. In the event of termination for convenience, the County will not receive reimbursement of pre-paid annual subscription fees for User ID's and Data Storage. In the event of such termination by the County, Riskconnect will perform all scheduled Services through the effective date of termination. In the event County provides the Termination Notice for convenience within forty-five (45) days of the subsequent contract year, then County shall be responsible for any subscription license fees that Riskconnect actually incurs related to the next renewal or subscription term.

22. County Right to Terminate: Notwithstanding anything to the contrary herein, the County shall have 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 Section, 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 Section, 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 terminated by the County for its convenience, 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.

23. Termination By Riskconnect: Riskconnect may terminate this Agreement solely if: (a) the County has failed to make payments due and payable hereunder, (b) the aggregate total of such payments exceeds Fifty Thousand Dollars (\$50,000), (c) such payment is not subject to a good faith dispute, (d) Riskconnect provides County with a minimum of thirty (30) days written notice after the

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.

- 24. Termination by the County for Non-Appropriation:** 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 the County. Riskonnect 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.
- 25. Orderly Termination:** 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, Riskonnect 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.
- 26. Force Majeure:** While not relieving Riskonnect of its duty to provide redundancy or establish backup and disaster recovery procedures as provided elsewhere in this Contract or its Exhibits or Schedules, no party to this Agreement 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 any Exhibit or Schedule 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) days, or be expected to last for a period of more than thirty (30) days, the party not relying on the excusable delay, at its option, may Terminate this Agreement as it relates to the Exhibit or Schedule involved.
- 27. 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.
- 28. 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.
- 29. Documentation/Meetings:** Riskonnect shall develop relevant documents necessary to complete the services and requirements as set forth in this Contract. The County's Project Manager and Riskonnect's Project Manager shall meet [by telephone is acceptable] on reasonable notice to discuss Riskonnect's performance and progress under this Contract. If requested, Riskonnect's Project Manager and other project personnel shall attend all meetings. Riskonnect shall provide such information that is requested by the County for the purpose of monitoring progress under this Contract.
- 30. Conflict of Interest:** The County's policies expressly prohibit it and its employees from engaging in activities involving a conflict of interest. Riskonnect 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 Riskonnect's performance of the Services hereunder. Riskonnect shall at all times exercise reasonable care and diligence to prevent any actions, circumstances, or conditions that could result in a conflict between Riskonnect (or any of its employees, agents, or subcontractors) and the best interests of the County. Such efforts by Riskonnect 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.
- 31. Confidentiality:** Riskonnect 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 restricts access to County Data to Riskconnect employees, affiliates' employees, or others who need to know that information to provide services to you or in the course of conducting our normal business operations. Riskconnect maintains appropriate physical, electronic, and procedural safeguards to protect County Data as governed in this Contract. Riskconnect shall protect data about the 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 I attached hereto and incorporated herein by reference. If County do provide Riskconnect with County Data, Riskconnect will only use it for the purposes described in this Agreement, and Riskconnect will 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 our contracted service providers or agents to provide services for Riskconnect; (3) in order 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 survivor; 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 Agreement.
- 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. 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 the County is subject to the requirements of the California Public Records Act. To the extent the County receives a request for Riskconnect Confidential Information; the 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, the 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.

32. 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 in this Section below) solely to the extent Riskconnect requires such access and use in order to properly and appropriately perform the Services as contemplated by this Contract. Riskconnect 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 it 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 of 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.

33. Audits/Inspections: At County's sole expense and 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.

34. 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.

35. 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.

- 36. 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 prior to go live. 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

- 37. Progress Reports:** Riskconnect shall provide to County a weekly written report as to the progress of completion of the activities contained in the Implementation Plan until each of Riskconnect's responsibilities thereunder have been completed. Such reports shall be in a format and include such detail as County may reasonably request.

- 38. Issue Management and Action Plan:** Riskconnect shall be responsible for identifying, analyzing, managing and recording issues and risks throughout the Implementation period and will provide County with an action plan for resolution.

- 39. 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.

- 40. Security Management Services:** Riskconnect shall provide appropriate and comprehensive security Services, that meet the County’s security requirements identified in Schedule A, 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.
- 41. 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 the Scope of Work. 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.
- 42. 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 in accordance with the frequency set forth in Schedule A. 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.
- 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 follow the processes established in Attachment G 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. Anti-Malware Protections: The 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 Section.

45. 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.

46. 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.

47. 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.

48. County and Riskconnect Project Manager: 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 County personnel interface with Riskconnect 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 shall be subject to approval by the 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 from providing services to the County under this Contract. The County's Project Manager shall notify Riskconnect in writing of such action. Riskconnect shall accomplish the removal within three (3) calendar days after written notice by the County's Project Manager. The County is 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 the County under this Contract.

49. Contactor Staff: In addition to the rights set forth in Section 48, County and Riskconnect Project Manager, above; the County's Project Manager shall have the right to require the removal and replacement of any of Riskconnect's personnel from providing services to the County under this Contract. The County's Project Manager shall notify Riskconnect's Project Manager in writing of such action. Riskconnect shall accomplish the removal of the specified personnel within one (1) calendar day after written notice by the County's Project Manager. The County is not required to provide any reason, rationale or factual information in the event it elects to request the removal of any of Riskconnect's personnel from providing services to the County under this Contract.

- 50. Riskonnect's Relationship Manager:** Riskonnect represents that the individual designated as Riskonnect'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, Riskonnect's Relationship Manager. Without the prior written consent of the County's Program Manager which consent shall not be unreasonably withheld, Riskonnect shall not: (a) designate a replacement for Riskonnect's Relationship Manager; or (b) voluntarily replace or reassign the individual serving as Riskonnect's Relationship Manager during the first twelve (12) months after the date that such individual commences performing the duties of Riskonnect's Relationship Manager hereunder. Riskonnect's Relationship Manager shall at all times: (i) act as the primary liaison between Riskonnect and the County's Relationship Manager; (ii) have overall responsibility for directing all of Riskonnect'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 Riskonnect'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 Riskonnect's performance under this Contract.
- 51. Additional Personnel Requirements:** Riskonnect shall, at all times, make available appropriate and sufficient numbers and types of Riskonnect Personnel, in addition to Riskonnect's Relationship Manager, to timely perform Riskonnect's obligations hereunder, in accordance with this Contract and all Attachments hereto.
- 52. Qualified Personnel:** In the event that Riskonnect fails to meet any of its obligations with respect to the required proficiency of any Riskonnect Personnel, Riskonnect shall promptly, as directed by the County, either: (a) take such action with respect to such Riskonnect Personnel, including promptly providing appropriate training, education, or orientation, as necessary for such Riskonnect Personnel to meet the applicable requirements set forth in this paragraph; or (b) in the event that the County has notified Riskonnect that such Riskonnect Personnel does not meet the applicable requirements, remove and replace such Riskonnect 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.
- 53. Employee Eligibility Verification:** Riskonnect 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. Riskonnect 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. Riskonnect shall retain all such documentation for all covered employees for the period prescribed by the law. Riskonnect 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 Riskonnect 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.
- 54. Employee Qualification and Verification:** Subject to and in accordance with applicable law, Riskonnect, prior to assigning an individual as Riskonnect Personnel and at Riskonnect'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, Riskonnect will certify in writing to the County that each and every employee of Riskonnect 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.
- 55. Training:** Riskonnect shall provide, and cause its subcontractors to provide throughout the Term of this Contract, all such technical and interpersonal training to Riskonnect Personnel, and to any employees of Riskonnect's subcontractors that are assigned to provide Services hereunder, as may be necessary and appropriate for them to collectively perform, on behalf of Riskonnect, all of Riskonnect's duties under this Contract. In any event, the levels and extent of training provided by Riskonnect to the Riskonnect Personnel shall be at least equal to the average levels of training given to other Riskonnect employees holding comparable positions, under similar circumstances, and performing work of a similar nature and level of complexity.

- 56. The County's Relationship Manager:** The 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.
- 57. 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.
- 58. Authority Retained By County:** The 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.
- 59. Set-Off:** The 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.
- 60. Disputed Amounts:** The 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.
- 61. 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 the 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 the 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.
- 62. County Payment upon Termination:** Riskconnect shall submit a final completion cost or credit invoice upon any termination of the Term by the County for convenience, pursuant to Section 21, or for non-appropriation, pursuant to Section 24 hereof. Upon approval of such final invoice, and subject to Riskconnect's compliance with all material terms and conditions of this Contract, the County shall promptly make payment of any remaining amounts due and payable to Riskconnect for Services rendered, provided, in the case of Termination under Section 24, that the final invoice does not contain any amounts attributable to the County Fiscal Year for which appropriations are not made.

- 63. 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.
- 64. Additional Licensing Provisions - Backup Requirement:** 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.
- 65. Data Load Requirements:** 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 Section 2 (Scope of Work) of 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 via using an encrypted secure FTP or secure web service protocol; and
 - 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.
- 66. 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 Attached hereto as Attachments L and M 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:
- 67. 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 K) and Data Classification Policy (Attachment L), as modified, supplemented, or replaced by the County or 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. Riskonnect shall, and shall cause the Riskonnect Personnel and subcontractors to, fully comply with and abide by all such Security Policies at all times during the Term.

- 68. Information Access:** Riskonnect 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, Riskonnect shall, and shall cause the Riskonnect 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. Riskonnect shall, and shall cause the Riskonnect 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 Riskonnect shall issue, any necessary information-access mechanisms, including access IDs and passwords, and in no event shall Riskonnect permit any such mechanisms to be shared or used by other than the individual Riskonnect Person to whom issued. Riskonnect shall provide each Riskonnect 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, Riskonnect shall provide the County with an accurate, up-to-date list of those Riskonnect Personnel having access to the RCMIS Systems, or County Data, and the respective security level or clearance assigned to each such Riskonnect Person. All RCMIS Systems, and all data contained therein, including County Data, used or accessed by Riskonnect Personnel: (a) shall be used and accessed by such Riskonnect Personnel solely and exclusively in the performance of their assigned duties in connection with, and in furtherance of, the performance of Riskonnect's obligations hereunder; and (b) shall not be used or accessed except as expressly permitted hereunder, or commercially exploited in any manner whatsoever, by Riskonnect, the Riskonnect Personnel or any subcontractor, at any time. Riskonnect acknowledges and agrees that any failure to comply with the provisions of this Section shall constitute a breach of this Contract and entitle the County to deny or restrict the rights of such non-complying Riskonnect Personnel to access and use the RCMIS Systems and County Data, as the County in its sole discretion shall deem appropriate.
- 69. 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 Riskonnect 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 Riskonnect shall be required to implement and enforce, as well as the date on which such procedures and measures shall take effect. Riskonnect shall, and shall cause the Riskonnect Personnel and subcontractors to, fully comply with and abide by all such enhanced security and access measures and procedures as of such date.
- 70. General Security Standards:** At all times during the Term, Riskonnect shall maintain a level of security with regard to the RCMIS Systems and County Data for which Riskonnect 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 Riskonnect 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.
- 71. Breach of Security:** Any material breach or violation by Riskonnect 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 Riskonnect under this Contract, and any chronic or critical breach by Riskonnect 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 Riskonnect under this Contract. .
- 72. 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 ensure all pertinent County security standards as well as any customer agency requirements, such as federal tax requirements. Riskonnect shall inform County of any security audit or assessment performed that includes County hosted content, within sixty (60) days of such audit or assessment.
- 73. Preparation for Successor to this Contract:** At any time or times during the Term, at the written request of the County, Riskonnect 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.

- 74. 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.
- 75. 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 Section. 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.

For RISKCONNECT.:

Riskconnect Inc.

ATTN: Jack S. Tatum
 Vice President – Global Business Development
 Phone: 770-790-4626
 Email: jack.tatum@riskconnect.com

For COUNTY:

Project Management

County of Orange, Risk Management
 ATTN: Tom Phillips
 Risk Manager
 Phone: (714)-285-5510
 Email: tom.phillips@ocgov.com

County Contract Administration

County of Orange
 County Procurement Office
 1300 S. Grand Ave. Building A, 2nd Floor
 Santa Ana, CA 92705
 ATTN: **Karen Vu**
 Supervising PCS
 Email: Karen.Vu@ocgov.com

- 76. 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 Section shall not be exclusive and are in addition to any other rights and remedies provided by law or under this Contract.
- 77. Publication:** No copies of sketches, schedules, written documents, computer based data, photographs, maps or graphs, including graphic art work, 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.

- 78. County of Orange Child Support Enforcement Requirements:** Riskonnect and its officers collectively certify compliance with (1) any and all court orders pertaining to child support and (2) all applicable federal and state reporting requirements pertaining to child support.
- 79. Change of Ownership:** Riskonnect agrees that if there is a change or transfer in ownership of Riskonnect's business prior to completion of this Contract, the new owners shall be required under terms of sale or other transfer to assume Riskonnect's duties and obligations contained in this Contract and complete them to the satisfaction of County.
- 80. Independent Contractor:** Riskonnect shall be considered an independent Contractor, and neither Riskonnect, its employees nor anyone working under Riskonnect shall be considered an agent or an employee of County. Neither Riskonnect, its employees nor anyone working under Riskonnect, shall qualify for workers' compensation or other fringe benefits of any kind through County.
- 81. Assignment or Subcontracting:** 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 Riskonnect 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.
- 82. Non-Discrimination:** In the performance of this Contract, Riskonnect 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. Riskonnect acknowledges that a violation of this provision shall subject Riskonnect 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.
- 83. Waiver of Jury Trial:** To the extent enforceable under California law, each Party acknowledges that it is aware of and has had the opportunity to seek advice of counsel of its choice with respect to its rights to trial by jury, and each Party, for itself and its successors, creditors, and assigns, does hereby expressly and knowingly waive and release all such rights to trial by jury in any action, proceeding or counterclaim brought by any Party hereto against the other (and/or against its officers, directors, employees, agents, or subsidiary or affiliated entities) on or with regard to any matters whatsoever arising out of or in any way connected with this Contract and/or any other claim of injury or damage.
- 84. 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.
- 85. 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.
- 86. Calendar Days:** Any reference to the word "day" or "days" herein shall mean calendar day or calendar days, respectively, unless otherwise expressly provided.
- 87. 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.
- 88. Attorney's 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.
- 89. 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.

90. 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.

91. Definitions:

A. *Software.* The term “Software” shall mean the 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” or “Services” shall mean the services required to be performed by Riskconnect in accordance with Section 2.

C. *Update.* The term “Update” shall mean any bugs, patches, fixes, enhancements, improvements to the Software and any addition of new features pertaining only to the County’s existing modules.

D. *Upgrade.* The term “Upgrade” shall mean platform changes, addition of new modules or new integration points or the creation of new versions.

E. *Documentation.* The term “Documentation” shall mean all written and electronic manuals, training material, or other associated printed materials and updated versions, which may be necessary or useful to the County in its use of the Software provided hereunder including all requirements set forth in the Terms and Conditions of this Contract.

F. *Annual Maintenance and Support or Software Annual Maintenance and Support.* The terms “Annual Maintenance and Support” or “Software Annual Maintenance and Support” shall mean the services set forth in Attachment G of the Contract

G. *Annual Maintenance and Support Period.* The term “Annual Maintenance and Support Period” shall mean the twelve (12) month consecutive period commencing on the Effective Date of the Contract. Each successive Annual Maintenance and Support Period shall commence at 12:00 midnight of the day of the expiration of the prior period.

H. *Acceptance Testing.* The term “Acceptance Testing” shall have the meaning set forth in Section 47 in the Terms and Conditions.

I. *Availability.* Except for planned or emergency maintenance, the term “Availability” means the percentage of time that the Riskconnect Service is fully operational and available to County in accordance with the Service Level Agreement found in Attachment G attached hereto.

J. *“Business Day”* means any day on which the County of Orange is open for business.

K. *“Change(s)”* means any change, modification, action or decision with respect to the Services.

L. *“User(s)”* means County employees, representatives, consultants, contractors, agents or third parties who are authorized to use the Riskconnect Service and have been supplied user identifications and passwords by County or by Riskconnect at County’s request.

M. *“County Data”* means the information or material that County submits, uploads, or transfers to the Riskconnect Service.

N. *“Effective Date”* had the meaning attributed to it in the first paragraph of this Contract.

O. *“Force Majeure Event”* means a cause beyond the reasonable control of a Party that materially prevents or delays such Party’s performance hereunder (or that materially affects such Party’s need for, ability to effectively utilize, or ability to provide, Services hereunder), including acts of God, act of governmental body or military authority, fire, explosion, power failure, flood, epidemic, riot or civil disturbance, war, sabotage, accidents, civil insurrections, blockades, embargoes, storms, labor disputes (except those involving personnel of Riskconnect or its subcontractors), earthquakes, elements of nature, terrorism, rebellions or revolutions in the United States, or other similar events. In no event will failure to meet Riskconnect’s Disaster Recovery requirements constitute a Force Majeure Event.

P. *“RCMIS”* means Risk and Claims Management Information System, otherwise referred herein as the Riskconnect Service.

Q. "*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;

R. "*Riskconnect Service*" means County's specific configuration of Riskconnect's web-based RCMIS Software identified and further defined in the "The Statement of Work", attached hereto and accessible via <http://www.riskconnect.com> or another designated web site or IP address, or ancillary online or offline products and services provided to County by Riskconnect, to which the County is being granted access under this Contract.

S. "*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.

T. "*Incident Resolution*" means the point at which Riskconnect has responded to an Incident and/or Problem and Riskconnect has either: (a) successfully diagnosed and taken appropriate corrective actions to return the systems(s) or service(s) to an acceptable level of operability and performance to the County to conduct business (including conducting and concluding a Root Cause Analysis as required); or (b) has provided an appropriate answer to an inquiry or an informational question that is understood by and acceptable to the County. In both cases, the Incident is not resolved until the County is convinced and satisfied that it has been resolved.

U. "*Maintenance Window*" is a County-approved period of time during which preventive maintenance that could cause disruption of service may be performed. SLR calculations exclude Maintenance Windows.

V. "*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.

W. "*Party*" or "*Parties*" shall have the meaning attributed to them in the first paragraph of this Contract.

X. "*Problem*" means a condition often identified as a result of multiple Incidents that exhibit common symptoms. Problems can also be identified from a single significant Incident, indicative of a single error, for which the cause is unknown, but for which the impact is significant.

Y. "*Reporting Period*" means all reports are provided on a monthly basis, within three (3) Business Days of the close of the calendar month, unless stated otherwise.

Z. "*Resolve*" or "*Resolution*" means 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. Implementing a Workaround is a partial or temporary resolution.

Contract Signature Page

The Parties hereto have executed this Contract on the dates shown opposite their respective signatures below

RISKONNECT INC.*:

Signature #1:

 Jack S. Tatum

Print Name:

Jack S. Tatum

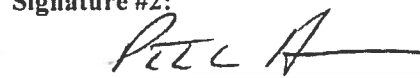
Title:

Vice President of Global Business Development

Date:

11/22/2013

Signature #2:

 _____

Print Name:

Patrick Henn

Title:

Chief Financial Officer

Date:

11/22/2013

* If the contracting party is a corporation, (2) two signatures are required as further set forth in this paragraph. The first signature shall be (a) the Chairman of the Board; b) the President; or c) any Vice President. The second signature shall be a) the Secretary; or 2) any Assistant Secretary; or 3) the Chief Financial Officer; or d) any Assistant Treasurer.

COUNTY OF ORANGE

A political subdivision of the State of California

By _____

Date _____

Approved by Board of Supervisors on: _____

APPROVED AS TO FORM
OFFICE OF THE COUNTY COUNSEL

By 

Deputy

County of Orange

Contract MA-017-14010752

ATTACHMENT A

SCOPE OF WORK

MASTER AGREEMENT MA-017-14010752

Scope of Work Objectives

Riskconnect's RCMIS Services is a cloud-based Software-as-a-Service solution known as the Riskconnect Service that will provide the County:

- a. A scalable and flexible platform that can be configured to manage risk-related needs
- b. A centralized database and analytics solution
- c. An environment to create, modify and manage screen design, security, workflow rules, and other system customizations necessary for the day-to-day use of the application

Upon Riskconnect's completion of the deliverables in this Contract, the following capabilities of the County's current Liability Claims Management System (LCMS) will be migrated to the Riskconnect RCMIS. Riskconnect's RCMIS Services will provide the County the:

- a. Ability to adjudicate auto and general liability claims
- b. Ability to adjudicate auto physical damage and first party property claims
- c. Ability to generate check requests for sending to Auditor/Controller
- d. Ability to attach document and photos to claim and litigation records
- e. Ability to manage and track subrogation
- f. Ability to produce reports for actuarial studies
- g. Ability to automatically import/integrate data from the County's CAPS+ financial system

The specific objectives for this Scope of Work include:

- a. Self-administration of specified claim coverages
- b. Financial, analytical and loss prevention trending reports and dashboards as well as claims reports for actuarial studies
- c. Workflow automation for adjudication and department activities
- d. Managing and tracking litigation
- e. Managing and tracking subrogation

Scope of Work Details

Table 1

USER LICENSES TYPES FOR RISK MANAGEMENT STAFF		In Scope
User License Type		Number of User Licenses
Platform Administrative Users (RCMIS)		2
Riskconnect Data Manager User (No Charge)		1
Platform Full Users		6
Incident Management Portal User (No Charge)		0

Operations Users (with Reports)	2
Operations Users	3
Riskconnect Business Intelligence Report Studio	0
Riskconnect Business Intelligence Business Insights Advanced	3
Riskconnect Business Intelligence Report Consumer	0
Certificates of Insurance	0
A.M. Best	0
Managed Disability Guidelines	0
Riskconnect Alerts	0

User access is provisioned at the time of initial system setup. The County will be invoiced based upon the number and type of licenses provisioned. Initial invoicing will be based upon the number and type of licenses noted in Table 1 above.

Table 2

RISKONNECT FUNCTIONALITY BY LICENSE TYPE					
Capability	Administrator	Full		Operations	Operations with Reports
Data Access					
Create, Read, Update and Delete (subject to Security Settings)	X	X		X	X
Views - Create and Edit	X	X			
Views - Run, Resort, Print	X	X		X	X
Basic, Brandable interface, look and feel				X	X
Mobile Applications Availability	X	X			
Inline Editing in Views	X	X			
Offline Briefcase	X	X			
Basic Document Management	X	X		X	X
Reporting and Dashboards					
Ad-Hoc Reporting - Edit filters and Share Reports	X	X			
Schedule reports	X				
Run on Demand Reports and Dashboards w/ Drill-downs	X	X			
Edit Report Filters	X	X			
Drag and Drop Dashboards	X	X			
Report and Dashboard Creation	X	X			
Run on Demand Reports (and drill) with predefined Filters Only (no run time prompts)					X
Receive Any Report Type via Email	X	X		X	X
Workflow					
Email Alerts	X	X		X	X
Task and calendar management	X	X			
Respond to/Manage own tasks	X	X			
Escalate for Approval	X	X			
Assign Tasks to Others	X	X			
Approve / Reject Authority	X	X			

Email template usage ("Send Email" Functionality)	X	X			
Administration and Configuration					
Create/Edit Views	X	X			
Create/Edit Letterhead & Email Templates	X				
Create/Edit Object and Field Configuration	X				
Create and Manage Workflows & Approvals	X				
Self-Service Data Loads	X				
Manage Full User Security	X				
Manage Operations User Access	X	X			
Other					
Chatter w/ Enhanced Document Management	X	X			
Enhanced Editable Grids	X	X			
Access to custom page layouts	X	X		X	X
Single-Sign-On Available	X	X		X	X
Riskconnect Data Manager User License is used by Riskconnect in the support of data integrations for our clients. There is no charge for this license type to the County of Orange.					

RISKCONNECT BUSINESS INTELLIGENCE FUNCTIONALITY BY LICENSE TYPE

Capability	Report Consumer	Business Insight Advanced	Report Studio	Mobile
CONSUME REPORTS				
Run Reports Interactively	X	X	X	
Access through Cognos Connection Portal to select and view reports	X	X	X	
Set personal preferences (for languages, time zones, etc.)	X	X	X	
Use the Cognos Connection Portal to create and consume portal pages	X	X	X	
Run and schedule reports	X	X	X	
Interact with report prompts	X	X	X	
Select report output formats such as HTML, EXCEL, PDF, and CSV	X	X	X	
Subscribe to and view scheduled reports	X	X	X	
Create and manage report folders and personalized standard reports	X	X	X	
AUTHOR REPORTS				
Utilize Cognos Search for dynamic and static text search of BI content		X	X	
Use the Business Insight module (advanced mode)		X	X	
Create Ad-Hoc reports		X	X	
Create Templates (in BIA)		X	X	
Create Templates (in Report Studio)			X	
Run Templates (and interact with prompts)	X	X	X	
Run OSHA Reports (and interact with prompts)	X	X	X	

Run Triangles (and interact with prompts)	X	X	X	
Consume Active Report Outputs		X	X	
Create Active Reports			X	
Distribute Active Reports			X	
Create Filters (in BIA)		X	X	
Create Filters (in RS)			X	
Run reports with filters already created	X	X	X	
Create Conditional Formatting (in BIA)		X	X	
Create Conditional Formatting (in RS)			X	
Run reports with Conditional Formatting already created	X	X	X	
Create Graphs and Enhanced Visualizations		X	X	
Run reports with Graphs and Enhanced Visualizations	X	X	X	
Create Maps		X	X	
Run reports with Maps	X	X	X	
Mobile		X	X	X
Burst Reports	X	X	X	
Consume Dashboards (and interact with prompts)		X	X	
Create Dashboards		X	X	
Drill down from dashboards		X	X	

TABLE 3

DATA STORAGE	In Scope
---------------------	-----------------

Existing County Data will be migrated from County systems to the Riskconnect RCMIS by Riskconnect. This Data includes:

Source	Type	Approximate Record Count
In-house LCMS and Others	Claims	25,000
In-house file systems	Files/images	120

County's Data Storage Subscription in the Riskconnect Service: The Riskconnect RCMIS will be configured with data storage capability of two (2) Gigabytes of storage for records (e.g., claims, incidents, hierarchy) and ten (10) Gigabytes for attachments (e.g., photos, witness statements). Additional data storage, if required, will be made available to the County at the rates noted in Attachment B, Section 10 Optional Services and Costs of this Scope of Work document. If County exceeds the amount of data or file storage subscribed by County in this SOW, County shall be charged excess data storage fees set forth in Attachment B, Section 10.

TABLE 4

RCMIS BASE CONFIGURATION	In Scope
---------------------------------	-----------------

A RCMIS database will be configured to accommodate all of the following:

Modules	Standard	Configurations specific to the County (Included in the Implementation Cost)
---------	----------	---

1. Location Hierarchy	Yes	Yes – as defined below
2a. Incidents	Yes	Yes – as defined below
2b. Claims	Yes	Yes – as defined below
3. Properties	Yes – as defined below	None included; County to use standard module
4. Exposures	Yes - as defined below	None included; County to use standard module
5. Policies	Yes – as defined below	None included; County to use standard module
6. Litigation/Matter Management	Yes	Yes – as defined below
7. Fleet	Yes – as defined below	None included; County to use standard module

1. LOCATION HIERARCHY

The Riskconnect RCMIS will provide the County with the following features or capabilities:

- a. The RCMIS database will include one (1) location hierarchy structure comprised of County departments which have zero, one or more Agencies which, in turn, have zero, one or more divisions.
- b. The hierarchy will be initialized by Riskconnect with an upload of a CSV file from the County.
- c. Ongoing location updates to the relationship between one agency/division and its parent in the hierarchy will be managed by Riskconnect Professional Services.

2. INCIDENTS AND CLAIMS

The Riskconnect RCMIS will provide the County with the following features or capabilities:

- a. The ability for the County to use codes for cause, nature, part and other coded / pick list fields similar to NCCI standard codes. County will provide most of the codes to Riskconnect and Riskconnect will be responsible for configuring the incidents and claim module as well as Riskconnect will provide standard values for some fields
- b. A configured claim object that features up to 50 specific fields including but not limited to:
 - i. Late indicator (not late, over 6 months and over 12 months) to be set by comparison of date claim received and date of loss
- c. Security and authentication features that allow:
 - i. Only authorized users to view, enter or change reserves
 - ii. Only authorized users to view, enter or adjust payments
- d. Standard classifications for risk reserves will include: bodily injury, medical, indemnity, property damage, expense and legal
- e. Standard aggregate classifications for pay codes including bodily injury, medical, indemnity, property damage, expense, legal and recovery
- f. Reserve transactions in excess of a given amount (to be determined during the implementation) will require an explanation upon entry
- g. Payments entered into Riskconnect will immediately impact claim financial reporting of total paid and remaining outstanding reserve. However, the payment will stay in Pending status until indicated as Complete with confirmation of feed from CAPS+. (See Data Interface Programming section)
- h. Within the payment process, the ability to generate a check request which is sent CAPS+
 - i. Riskconnect will ensure that check requests contain all fields/information required by the County Auditor/Controller and may be sent via paper mail or e-mail to the Auditor/Controller for payment. Special data fields for inclusion with each check request include:
 - ii. Riskconnect RCMIS must identify check payments where the Auditor/Controller must send the check back to Risk Management to be mailed
 - iii. Riskconnect RCMIS Specify payment as confidential.
- i. The ability for County-authorized users to adjust a payment as overpayment, duplicate or voided; each of these situations generates an adjusting transaction associated with the original transaction and is identified as an adjustment
- j. Subrogation functionality that includes fields for tracking the responsible third-party (with a lookup to Contacts), the reason for subrogation (text), statute date, subrogation status (from a pick list) and a currency field for estimated

damages to be recovered through subrogation. This estimated damages currency field is not part of the financial reporting. However, actual recoveries received are tracked as a claim transaction and will impact the calculation of net paid and net incurred.

- k. First Party Property Damage payments will be indicated as absorbed by the agency or excess of the deductible. Recoveries received excess of the deductible and are tracked and identifiable as from the carrier. These recoveries received are then reimbursed to the agencies as part of the County's normal transaction process.
- l. Claims will be associated with a Policy by the user picking the appropriate policy. Riskconnect will auto-populate the policy field in the instance where there is an absolute programmable rule on making the policy association (e.g., a John Wayne Airport (JWA) claim is a specific policy)
- m. The ability to have Claims associated with a Litigation Case by the User picking the appropriate case or creating a new litigation case and then make the association
- n. The ability to allow the adjuster to request a claim be submitted to ISO one-time or on a periodic basis as long as the claim is open
- o. Riskconnect will add a button on the claim page layout to locate the incident address on Google maps.
- p. Riskconnect will configure the Incident and Claims objects to account for:

Claim Component/Coverage Type	Claims Adjudication	Standard	Configurations specific to the County (Included in the Implementation Cost)
Workers Compensation	No	Yes	No
Auto Liability	Yes	Yes	Yes
Auto Physical Damage	Yes	Yes	Yes
General Liability	Yes	Yes	Yes
Subrogation	Yes	Yes	Yes
1st Party Property Damage	Yes	Yes	Yes

3. PROPERTIES

- a. County will use Riskconnect RCMIS to track property details including Construction, Occupancy, Protection and Environmental (COPE) information.
- b. County will use Riskconnect RCMIS to track property recommendations and to collect, store and report on property values.

4. EXPOSURES

- a. County will use Riskconnect RCMIS to track exposures such as headcount by Agency, payroll by Division, miles driven by Department, vehicles assigned by Agency, etc.
 - i. Exposure data is associated with some record in the location hierarchy and it can be at any level in the hierarchy
 - ii. Exposure data has an evaluation date

5. POLICIES

- a. County will use the Riskconnect RCMIS to track policy details including policy number, carrier, retention, effective date, expiration date, excess policy number and other fields for policy, policy section, policy subsection, policy endorsement, policy transaction and policy losses.

6. LITIGATION/MATTER MANAGEMENT

The Riskconnect RCMIS will provide the County with the following features or capabilities:

- a. User level security that will limit access to litigation records and associated documents to authorized users
- b. The ability to track all litigation dates including but not limited to: court dates, trial dates, MSC, MSJ and settlement dates
- c. The ability to track information about plaintiff and defense attorneys, jurisdiction, and court venues

- d. The ability to associate expenses, settlements and judgments with litigation and track these items as individual legal transactions in conjunction with the corresponding claim
- e. Reporting and dashboards that associate the litigation and claim data
- f. Contact management capability that stores attorney and judge details are stored in the Contacts object and in addition to standard contact fields, there is an approved contract attorney checkbox/picklist that for each contract attorney for each fiscal year.
- g. When entering attorney invoices for payment there will be a field to include the number of hours the attorney spent on a specific claim.

7. FLEET

The Riskconnect RCMIS will provide the County with the following features or capabilities per further instruction by County:

- a. The ability to store fleet data and to assign fleet vehicles to a department, agency or division
- b. The fields necessary for generating an auto schedule for policy renewal purposes

8. WORKFLOWS

- a. The Riskconnect System will be delivered with workflows, approval process and e-mail notifications using e-mail templates
- b. The workflows will be triggered by a data condition (e.g., new event report, property damage estimate in excess of \$5,000, liability claim with bodily injury paid, etc.) and the associated workflow automation can initiate any number of:
 - i. E-mail notification(s) – e-mail templates that will auto-populate with data from the record associated with the workflow rule
 - ii. Task assignment(s) to user(s) (e.g., escalate a claim for supervisor review)
 - iii. Field update(s) to some other related data (e.g., update a subrogation status field)
- c. Workflows for approval will include multiple layers of approval and will comply with standard platform approve/reject functionality.
- d. The Riskconnect System will be delivered with the following workflow rules, approvals, and e-mail templates to produce up to a total of 25 workflows, 5 approval process and 10 e-mail notifications with their associated email templates.

Workflow Rules and Actions	Approval Processes	E-mail Templates
<ul style="list-style-type: none"> If 6 or more months between date of loss and date claim received then do a field update of the late indicator and task to Unit Manager and file handler that claim is late (or too late if over 12 months) and appropriate letter must be sent out. 	<ul style="list-style-type: none"> Auto Approves Reserves under adjuster authority and manager approval needed above. Approval process for Reserve will display the explanation for the reserve change. 	<ul style="list-style-type: none"> Notification of significant reserve change (\$250K or more) or total incurred of \$500K or more
<ul style="list-style-type: none"> When a value is initially set for a litigation calendar date (e.g. MSC, mediation, appeal, etc.) then assign task to unit manager and adjuster. 	<ul style="list-style-type: none"> Approval Process for Payment that Exceeds Outstanding Reserves 	<ul style="list-style-type: none"> Notification of claim to report to excess carrier. Text to include incurred (\$2.5 million) and other qualifying criteria such as John Wayne Airport (JWA) or Immigration and Naturalization Service (INS).
<ul style="list-style-type: none"> When a litigation calendar date is changed then set new task for unit manager and adjuster to update their calendar 		<ul style="list-style-type: none"> Notify of a new claim
<ul style="list-style-type: none"> For Federal Litigation (district court) assign task for manager and file handler that within 21 days of service the court must respond with when addressed, when assigned and when accepted 		<ul style="list-style-type: none"> Notify of a liability claim with bodily injury payments
<ul style="list-style-type: none"> For Superior Litigation (superior court) assign task for manager and file handler that within 30 days of service the court must respond with when addressed, when assigned and when accepted 		
<ul style="list-style-type: none"> Upon entry of a new claim assign task to adjuster to set a reserve or explanation if no reserve (other than \$1) within 45 days and 		

assign task to adjuster to attach response letter (see Correspondence feature in Document Management section below) to the claim		
• Claims with Subrogation potential will assign a follow-up task to adjuster		
• Switch of an Incident to Open Claim will send e/m notification		
• Subrogation statute expires in 90 days notification sent to adjuster and manager		
• Claims that might be reportable to CMS send a notification to the manager		
• Notify manager for a payment issued amount from CAPS+ that differs from the corresponding check request amount.		

9. CHATTER

The Riskonnect RCMIS will provide the County with the following features or capabilities:

- a. The ability to follow users, properties, locations, claims, etc. to receive broadcast updates.
- b. The capability for users to form groups and post messages on each other's profiles to collaborate on projects

10. DOCUMENT MANAGEMENT

The Riskonnect RCMIS will provide the County with the following features or capabilities:

- a. The ability to store templates, presentations and videos
- b. The ability to subscribe to files and receive an e-mail notification when new versions are published or changes are made to the file's properties
- c. The ability for users to collaborate while maintaining version control
- d. The ability for users to create content packs for delivery of confidential documents to outside counsel
- e. Incoming email service will be configured for the Claim and Litigation objects for easy attachment of documents
- f. Riskonnect's RCMIS correspondence feature will be configured with the following statute letters or memos:
 - i. claim acknowledgement
 - ii. claim insufficient information
 - iii. claim denial
 - iv. claim filed too late
 - v. notification to appropriate department
- g. Riskonnect will provide documentation and training to County authorized user(s); this training will include how to configure additional letters

SECURITY CONFIGURATION

In Scope

Riskonnect RCMIS security configuration will limit user access to functionality (e.g., reports, dashboards, objects, tasks, calendars, etc.). The system will restrict granted access to view, create and edit capabilities. Riskonnect will configure County's RCMIS with the different profiles to enable user license types in Table 1 above. Additional profile(s), queue(s), role(s) or sharing model(s) will be configured to achieve the following security at no additional cost to the County.

1. Location Hierarchy maintenance
2. Claim transaction administration access, authority and approval for reserves and payments; this includes special rules for confidential transactions and transaction adjustments
3. Claim, Litigation and Subrogation access

DATA INTERFACE PROGRAMMING

In Scope

1. Riskconnect will load or extract data as per the details and specifications in the table below.
2. Riskconnect will be responsible for the execution, generation and reconciliation of verification reports such as control totals for all implementation and ongoing data interfaces. The County will work with Riskconnect to resolve verification issues.
3. Historical reserve transactions will be recreated by Riskconnect based upon payment data at the claim level, whenever such data is missing
4. The CAPS+ interface requires a reconciliation process.
 - a. That reconciliation can only be partially automated. For payments that match exactly based upon claim, invoice number and amount, the payment record will be updated with the check number and issue date.
 - b. For payments that are aggregated to a payee and in aggregate match on claim, invoice number and amount, the payment records will be updated with the check number and issue date.
 - c. For single payments or payments aggregated by payee where there is not an exact match based upon claim, invoice number and amount, the data from CAPS+ will be made available for manual reconciliation by an authorized user.

11. Implementation Data Interface Requirements

Riskconnect has included the following interfaces in the implementation cost.

Interface Name	Inbound to RK or Outbound from RK or Bi-directional	Transmission (SFTP, manual upload, etc.)	Frequency (initialization/ one-time or on-going)	Type (historical transactions, snapshot, activity cumulative, etc.)	Source (TPA/Carrier, Client internal System, 3rd party Riskconnect, etc.)	Data (claims, transactions, adjuster notes, policies, etc.)
LCMS	Inbound	SFTP	One-time	Snapshot of Claim and Historical Payments	In-house MS Access	Claims and payments (no reserve transactions, no attachments)
Litigation Log	Inbound	SFTP	One-time	Snapshot	In-house MS Access	Litigated Cases
Diary	Inbound	SFTP	One-time	Snapshot	In-house MS Access	Diaries
Historical Reserves	Inbound	SFTP	One-time	Snapshot	In-house MS Access	Claim Reserve Amounts
CAPS+	Inbound	SFTP	On-going	Activity	In-house	Payments
ISO Query	Bi-directional	SFTP	On-going	Snapshot	3rd Party	Claims
ISO CMS	Bi-directional	SFTP	On-going	Activity & Transactional	CMS RRE	Liability Claims

12. Ongoing Data Interface Requirements

Riskconnect will ensure that the following interfaces are executed on-going as per the frequency column:

Interface Name	Inbound to RK or Outbound from RK or Bi-directional	Transmission (SFTP, web service, manual upload, etc.)	Frequency (daily, weekly, on demand, etc.)	Type (historical transactions, snapshot, activity cumulative, etc.)	Source / Destination (TPA/Carrier, Client internal System, 3rd party Riskconnect, etc.)	Data (claims, transactions, adjuster notes, policies, etc.)
----------------	---	---	--	---	---	---

CAPS+	Inbound	SFTP	Daily	Activity	In-house	Payments
ISO Query	Bi-directional	SFTP	Batch with schedule TDB	Snapshot	3rd Party	Claims
ISO Center for Medicare and Medicaid Services (CMS)	Bi-directional	SFTP	Monthly Queries & Quarterly Report Submissions	Activity & Transactional	CMS Responsible Reporting Entity	Liability Claims

REPORTS & DASHBOARDS	In Scope
---------------------------------	-----------------

Riskconnect will configure the following for Reports and Dashboards:

- The County provided samples of these reports where available and will work with Riskconnect to define any filtering or business rule logic needed for the reports.
- These following reports will be created by Riskconnect for the County or created in a training workshop and be available to the County at go-live.

Report Configuration Item
RCMIS Platform Report Build-out
COGNOS Report Build-Out
<p>Riskconnect RCMIS-provided Custom Reports</p> <ol style="list-style-type: none"> Report capability for reporting on contracting legal firms performance, claim handling costs, cases handled, settlements, and claim outcome. Report capability for reporting on contracting legal firms performance, claim handling costs, cases handled, settlements, and claim outcome. Report capability for cost of claims settled versus costs of lawsuits compared by the stages of the process. System provides a register of all open and closed litigated claims by contract defense firm. Subrogation recovery register: Report the number of claims subrogated, claims by status, recoveries and recovery success ratio by agency, coverage and adjuster. Financial Summary report of full value, SIR and excess only. CAPS+ unmatched payments report CAPS+ adjusted payments report

- Riskconnect will provide the County with the Standard Platform Reports Library
- County-authorized Full or Admin users will be trained by Riskconnect to create, modify, refresh, schedule and distribute dashboards using the standard Riskconnect dashboard functionality
- Historical reserves transactions will be recreated by Riskconnect based on payment data at claim level, whenever such data is missing
- Riskconnect will provide standard versions of Riskconnect Business Intelligence reports for OSHA 300 Reporting and Loss Triangles. The standard Loss Triangle have:
 - Parameters for: Triangle Type (annual, semi-annual, quarterly, monthly) and Triangle Period (calendar year, policy year, actuarial year, fiscal year, custom year)
 - Option for: Partial Ending Year, Starting Month, Claim or Occurrence, Combine Selected Coverages, Financial Capped Amount (limited), Development Factors, Financial Triangle Selection (e.g. net or gross, paid or incurred, total or by bucket such as medical, indemnity or expense)
 - Filters for: Date Start, Date End, Evaluation Date, Major Coverage, Minor Coverage, Carrier/TPA, Claim Status, Location Hierarchy, State, Cause

13. IT System Security Requirements:

Riskconnect will comply with the County and Riskconnect Security Policies and Procedures, and develop and execute security practices consistent with the Security Policies and Procedures provided by County. Without limitation to the foregoing, Riskconnect shall:

- Develop and maintain, as applicable to County, documented IT security processes and procedures that are in compliance with those provided by County.
- Provide all security policies and procedures to County for review and approval upon County's request and, at a minimum provide said policies and procedures quarterly for County's review and approval. All documentation shall be provided in electronic format for County's review.
- Comply with regulatory requirements as they relate to County's systems and data, which, as of the Effective Date, if applicable, include but are not limited to Health Insurance Portability and Accountability Act (HIPAA), SB1386 compliance, and Payment Card Industry (PCI),.
- Comply with County data classification, including County "Proprietary", "Confidential" and "Sensitive".
- Bear the cost of compliance for changed Security Policies and Procedures.
- Comply with reasonable requests by County for audits of security measures, including those related to ID and password administration.
- Comply with reasonable requests by County for physical inspections on site where Riskconnect provides Services.
- Provide County with any annual audit summaries and certifications, including but not limited to ISO or SOX audits.
- Designated a single point of contact to facilitate all IT security activities related to the services of this Contract. Such contact shall be available on a 7/24/365 basis.

14. IT Security – Physical Security and Access Control:

With respect to Riskconnect's facilities, Riskconnect shall comply with security requirements and establish processes and procedures that are set forth in this Contract and that are, at a minimum, consistent with best practices.

15. IT Security – Training and Compliance:

Riskconnect shall ensure that all employees providing Services are trained on security measures and practices, including, without limitation, County's Security Policies and Procedures, as may be updated by County from time to time. The cost of providing training shall be borne by Riskconnect

Riskconnect shall ensure that all employees providing Services comply with the Security Policies and Procedures, and shall take all reasonable measures to reduce the opportunity for unauthorized access, transmission, modification or misuse of County's data by employees providing Services. At a minimum, Riskconnect shall:

- Ensure that a formal disciplinary process is defined and followed for employees providing Services violating the Security Policies and Procedures.
- Proactively manage and administer access rights to any equipment, software and systems used to provide services to County.
- Define, maintain and monitor access controls, ranging from physical access to logical security access, including a monthly review of employees' providing Services access to facilities and systems used to provide Services to County.

Riskconnect shall monitor facilities, systems and equipment to protect against unauthorized access. Riskconnect will:

- Monitor access to systems, investigate apparent security violations and notify the County of such, per the County's notification requirements, including routine reporting on hacking attempts, penetrations and responses.
- Maintain data access control and auditing software, and provide adequate logging, monitoring, and investigation of unusual or suspicious activity.
- Initiate immediate corrective actions to minimize and prevent the reoccurrence of attempted or actual security violations.
- Document details related to attempted or actual security violations and provide documentation to County.
- Provide necessary documentation and evidence to the County, per the County's requirements, in connection with any legal action or investigation.
- Ensure that all equipment used to provide Services to County shall have anti-virus software with the latest patches installed.

16. County Responsibilities:

County users must be on one of the following supported browser versions:

- Microsoft Internet Explorer versions 7, 8, 9, 10 or up to the most recent stable version
- Mozilla Firefox most recent stable version
- Google Chrome most recent stable version
- Apple Safari version 5.1.x on Mac OS X or up to the most recent stable version

County users with Cognos Business Insights Advanced (BIA) or Report Studio licenses must be on one of the following supported browser versions:

- Microsoft Internet Explorer versions 7, 8, 9 and 10
- Mozilla Firefox most recent stable version

Ongoing location updates will be managed directly by County with the exclusion of updates to the relationship between one agency/division and its parent in the hierarchy.

For coded fields (e.g. cause, nature, part, etc.) County will provide the codes values to be used.

17. Project Management/Team Responsibilities

- The following County roles & responsibilities have been identified in order to timely complete the implementation tasks specified in this Statement of Work.

County Risk Manager
<ul style="list-style-type: none"> • Serve as the executive point of contact with Riskconnect during the performance of this Statement of Work • Monitor the progress of Services associated with this Statement of Work • Participate in Kickoff Meeting • Attend training for Riskconnect RCMIS system • Work with the County Project Manager on critical decision making
County IT Project Manager
<ul style="list-style-type: none"> • Work as a single point of contact for the County Project team • Provide leadership and direction to the Project Team • Review Project progress with the Riskconnect Project Manager and resolve deviations from the project plan with Riskconnect's Project Manager • Support Project change control in accordance with defined Project Change Control Procedures • Participate in kickoff meeting, working meeting, and status calls • Coordinate access to representative end users, technology resources, and carrier contacts as needed • Provide input to training design and coordinate training logistics • Manage communication with Riskconnect
County Program Manager
<ul style="list-style-type: none"> • Manage communication and acceptance of deliverables with Riskconnect • Notify team of delays by Riskconnect
County Project Implementation Team
<ul style="list-style-type: none"> • Participate in kickoff meeting, working meetings and status calls • Provide input to Riskconnect RCMIS system design and configurations • Provide business rules, workflow, and necessary documentation for the new RCMIS system • Attend training for Riskconnect RCMIS system
County Risk Management

<ul style="list-style-type: none"> ● Participate in kickoff meeting ● Provide security standards documentation ● Assist with setup for training
County System Administrator(s) Responsibility
<ul style="list-style-type: none"> ● Maintain user lists and security ● Maintain report templates ● Perform regular data updates, if necessary ● Work with Riskonnect on system enhancement requests or any other administrator issues

18. Riskonnect Roles and Responsibilities

Riskonnect will provide the following resources for the project:

Riskonnect Senior Consultant & Project Manager
<ul style="list-style-type: none"> ● Work as single point of contact representing Riskonnect during system implementation ● Conduct weekly status meetings and create meeting minutes including necessary action items ● Work closely with the County Project Manager to resolve all issues ● Review project schedule and project resources with the County Project Manager ● Measure, track and evaluate progress of service deliverables and provide a weekly status report to the County Project Manager ● Resolve issues and maintain an issue log and report issue status to the County Project Manager ● Support change control in accordance with defined Project Change Control Procedures ● Manage all Riskonnect resources including the Riskonnect technical lead ● Support change control in accordance with defined Project Change Control Procedures ● Provide all deliverables in accordance with the defined dates during system implementation ● Transition the newly developed system to the on-going support team with Riskonnect's organization
Riskonnect's Technical Lead
<ul style="list-style-type: none"> ● Work as a technical lead for system design, integration of all components and overall implementation of the new system ● Develop design and Implementation plan and review with the County project team ● Work as a single point of contact for all technical issues ● Provide updates to the County Project Manager
Riskonnect's Service Analyst
<ul style="list-style-type: none"> ● Assist the Riskonnect project team in day-to-day tasks associated with the implementation of the Software ● Provide ongoing service and support
Riskonnect's Data Integration Specialist
<ul style="list-style-type: none"> ● Responsible for regular data processing activities after sign off on the conversions from the regular source(s)

ATTACHMENT B

COST/COMPENSATION FOR RISKONNECT'S SERVICES

MASTER AGREEMENT # MA-017-14010752

1. COMPENSATION

This is a fixed price Contract between the County and Riskonnect for the Services as set forth in this Contract. Riskonnect agrees to supply all Services as set forth in Section 2 of the Contract. Riskonnect agrees to accept the specified compensation as set forth in this Contract 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 until acceptance, for risks connected with the services, and for performance by Riskonnect of all its duties and obligations hereunder. The County shall have no obligation to pay any sum in excess of the amounts specified herein unless authorized by amendment.

2. SUBSCRIPTION FEES PAYABLE ANNUALLY IN ADVANCE

Following the Effective Date and on each anniversary of the Effective Date thereafter during the Term, following receipt of an acceptable invoice from Riskonnect, the County will pay in advance the following Subscription and Infrastructure /Processing fees.

Riskonnect Service Subscription Fees	\$ 49,719
Infrastructure and Processing Subscription	<u>\$ 9,700</u>
Total Subscription Fees to be paid in advance	\$ 59,419

3. IMPLEMENTATION PLAN MILESTONE PAYMENTS

Implementation Plan Payments totaling \$122,875 will be paid in three (3) installments—broken up into 40%, 30% and 30% installments--following the County's written acceptance of each Milestone specified below. For Milestone 1 below, the County shall pay Riskonnect \$49,150.00. For Milestone 2 below, the County shall pay Riskonnect \$36,862.50. For Milestone 3 below, the County shall pay Riskonnect \$36,862.50. For Milestone 2 and 3, if the County does not accept or reject by the agreed upon acceptance date of the delivery of said Milestones as set forth in the Implementation Plan Schedule, then County agrees to pay Riskonnect in good faith.

Payments will be made in 45 days after the County written acceptance of the Payment Milestones and subsequent receipt of an acceptable invoice from Riskonnect. Payment Milestone requirements are more fully specified in Attachment D – Implementation Plan.

Payment Milestone 1: Contract Execution, professional service team assigned and licenses provisioned (enabled) approved by the County

Payment Milestone 2: Shall occur upon County's acceptance testing (as provided in the Contract) of all deliverables leading to milestones DY8 and LL8 as set forth in the Implementation Plan of Attachment D.

Payment Milestone 3: Shall occur upon County's acceptance testing (as provided in the Contract) of all deliverables leading to milestone Prod 9 as set forth in the Implementation Plan of Attachment D.

4. PROFESSIONAL SERVICES AND SUPPORT FEES – PAID ANNUALLY AT FIRST ANNIVERSARY OF EFFECTIVE DATE IN ADVANCE

Upon the first anniversary of the Effective Date and each anniversary thereof during the Term, upon receipt of an acceptable invoice, the County will pay to Riskonnect:

50 Support hours	\$ 9,375
Ongoing Data Feeds	<u>\$ 14,500</u>

Total Annual Amount**\$ 23,875****5. TRAVEL EXPENSES**

During Implementation, the County will not be responsible for any travel and expense fees associated with the following visits:

- Project Kick-Off meetings – 2 days (back to back) for 2 people
- RCMIS Training Meetings – 2 days (back to back) for 2 people

If the County requests travel over and above the aforementioned on-site visits, the County will reimburse Riskconnect a daily meeting rate of \$3,000 (per person) for the first day of on-site meetings. Assuming back-to-back meetings, daily meeting rates for day 2 and beyond is \$1,500 / day per person. Riskconnect agrees for all on-site meetings to be pre-approved in advance, by the County Risk Manager. Sales and Executive team travel, which includes, but is not limited to the implementation kick-off meeting and one annual stewardship meeting, will not be billable to the County.

6. COUNTY PAYMENT TERMS

Riskconnect shall reference Master Agreement # MA-017-14010752 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 rests 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

Invoices and support documentation must be forwarded to:

County – Risk Management
600 W. Santa Ana Blvd., Suite 104
Santa Ana, CA 92701
Attention: Risk Manager

8. IMPLEMENTATION COST DETAILS

One-Time implementation Fees for Riskconnect RMIS

One-time Professional Services Fees	
	One-Time Total
RMIS Project Management	\$ 5,625.00
RMIS Configuration	\$ 37,500.00
RMIS Custom Reports	\$ 12,000.00
Location Hierarchy and Security	\$ 3,750.00
Implementation Kick-Off Meeting - Day 1 (2 Riskonnect attendees)	\$ 6,000.00
Implementation Kids-Off Meeting - Day 2 (2 Riskonnect attendees)	\$ 3,000.00
Training and Go-Live Meeting - Day 1(2 Riskonnect attendees)	\$ 6,000.00
Training and Go-Live Meeting - Day 2 (2 Riskonnect attendees)	\$ 3,000.00
Total One-time Professional Services Fees	\$ 76,875.00
One-Time Data Services Fees	
LCMS	\$ 12,500.00
Litigation Log	\$ 5,000.00
Diary	\$ 7,500.00
Historical Reserves	\$ 7,500.00
CAPS+	\$ 10,000.00
ISO Query	\$ 1,500.00
ISO CMS	\$ 2,000.00
Total One-Time Data Services Fees	\$ 46,000.00
Total One-Time Implementation Fees for Riskonnect RMIS	\$ 122,875.00

9. ANNUAL RCMIS FEES FOR LICENSES, DATA STORAGE AND SERVICES

On-going Annual Fees for Riskonnect RCMIS			
Annual Licensing Fees			
	Units / Hours	Rate per Unit	One-Time Total
System Admin. - RCMIS	2	\$ 8,400.00	\$ 16,800.00
Full User	6	\$ 4,550.00	\$ 27,300.00
Operations with Reports	2	\$ 360.00	\$ 720.00
Operations	3	\$ 263.00	\$ 789.00

Business Intelligence - Business Insights Advanced	3	\$ 1,370.00	\$ 4,110.00
Total Annual Licensing Fees			\$ 49,719.00
Infrastructure and Processing			
Data (GB)	2	\$ 4,250.00	\$ 8,500.00
Attachments (GB)	10	\$ 120.00	\$ 1,200.00
Total Annual Infrastructure and Processing			\$ 9,700.00
Professional Services			
Support Services	50	\$ 187.50	\$ 9,375.00
Data Services			
CAPS+	Daily	\$ 7,500.00	\$ 7,500.00
ISO Query	Batch Schedule	\$ 3,500.00	\$ 3,500.00
ISO CMS	Monthly Queries and Quarterly Report Submissions	\$ 3,500.00	\$ 3,500.00
Total Annual Professional Services			\$ 23,875.00
Total On-going Annual Fees for Riskonnect RCMIS		\$	83,294.00

10. OPTIONAL SERVICES AND COST

The County may optionally add additional RCMIS licenses up to the maximum amount noted below at the following pre-negotiated costs.

User License Type	Maximum 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
Riskonnect Business Intelligence Report Studio	3	\$2,630
Riskonnect Business Intelligence Business Insights Advanced	5	\$1,370
Riskonnect Business Intelligence Report Consumer	5	\$840

The County may add additional data storage up to the maximum amount noted in the table below at the following pre-negotiated costs. If County exceeds the amount of data or file storage subscribed by County in Table 3 of Attachment A, County shall be charged excess data storage fees set forth below.

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

Attachment storage fee	\$120
------------------------	-------

The County may optionally 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

The County may optionally add additional Professional Support Services at the rates noted in the table below. Optional Professional Support Service hours will be invoiced monthly on a time and expense basis.

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

ATTACHMENT C

RISKCONNECT'S STAFFING PLAN

Master Agreement MA-017-14010752

A. IMPLEMENTATION TEAM

NAME	ROLE	RESPONSIBILITIES
Josh McJenkin	Regional Director, West	Responsible for all Riskconnect personnel and service delivery to endure a successful implementation of the deliverables set forth in Attachment A – Scope of Work
Michael Banks	Project Manager	Primary point of contact for all County needs throughout the implementation. Responsible for developing and managing the project schedule, coordinating project work, identifying and removing roadblocks for a successful implementation.
Justin Gates	Platform Consultant	Installs managed packages, product suites and modules. Configures objects and fields, creates automation such as workflows and approvals based on Risk Managements specifications. Provisions the platform, licenses and storage.
Meredith Randall and Steve Powell	Business Consultants	Responsible for gathering system requirements, documenting the County's business process, applying Riskconnect industry-based best practices, building a solution design, configuring a system

		that meets the County's needs and providing functional enablement to the County Risk Management.
Henry LaFon and Rick Parks	Data Consultant	Responsible for the data architecture plan and data integration which includes requesting data from various third-party Riskconnect, communicating data standards to all providers, mapping data fields to database elements, instantiating standard data imports, performing data imports and extracts.
Elizabeth Morrell	Training Consultant	Delivers product training for suites and modules. Also delivers user-specific training for the Risk Management system administrators, County business intelligence analysts and other licensed users. Provides general knowledge transfer about the platform and best practices.
Dandan Yang	Business Intelligence Consultant	Responsible for gathering reporting requirements, designing, building and deploying reports and dashboards to maximize business intelligence across various reporting platforms.

B. POST "GO-LIVE" SUPPORT TEAM

NAME	ROLE	RESPONSIBILITIES
Josh McJenkin	Regional Director, West	Responsible for all Riskconnect personnel and service delivery to endure a successful implementation of the deliverables set forth in Attachment A – Scope of Work
Justin Gates	Platform Consultant	Installs managed packages, product suites and modules. Configures objects and fields, creates automation such as workflows and approvals based on Risk Managements specifications. Provisions the platform, licenses and storage.

ATTACHMENT D

IMPLEMENTATION PLAN, ACCEPTANCE AND TESTING PROCEDURES

Contract MA-017-14010752

The following Implementation Plan is expected to take a maximum of seven (7) months from the Effective Date unless otherwise agreed to by the County Risk Manager. The Parties agree to work diligently to accomplish all aspects of the Implementation Plan within the prescribed time.

Riskconnect Implementation Plan

Task		Responsible	Expected Start Week after Contract Execution	Target Completion Week after Contract Execution	Project Plan and Payment Milestones	Dependencies
Administrative						
A1	Contract Execution	County and Riskconnect	Week 0	Week 0		
A2	Assign County Service Team	Riskconnect	Week 1	Week 1		A1
A3	Project Kickoff Call	County and Riskconnect	Week 1	Week 1	Milestone	A2
A4	Request Legacy, TPA & Internal Data Information	Riskconnect to provide Documents to County. County forwards to internal IT and Riskconnect	Week 1	Week 1		A3
A5	Contract Execution, professional service team assigned and licenses provisioned (enabled)	Riskconnect	Week 1	Week 1		A1
A6	Project 2-day face-to-face kick-off meeting with substantial time in the system with user review	County and Riskconnect	Week 1	Week 2	Milestone	A3
A7	Establish shared baseline project plan in Riskconnect system	Riskconnect	Week 2	Week 2		A3
A8	County Approval of Baseline Project Plan	County	Week 2	Week 2	Payment Milestone #1	A6
County Hierarchy						
H1	Design meeting for hierarchy structure and initialization file	County and Riskconnect	Week 2	Week 2		A3 - agenda item for A6
H2	Prepare hierarchy file and deliver to RK	County	Week 2	Week 3	Milestone	H1
H3	Riskconnect Acceptance of County hierarchy file	Riskconnect	Week 3	Week 3	Milestone	H2. Assumes that hierarchy file conforms to RK

						standards and is in format ready for load
H4	Configure for hierarchy	Riskconnect	Week 3	Week 3		H2
H5	Analyze hierarchy and load to RK	Riskconnect	Week 3	Week 4		H3
H6	Review and approve hierarchy in RK	County	Week 4	Week 4	Milestone	H4, H5
Self-Administration including Subrogation for Auto and General Liability, (1st & 3rd Party) Property and Auto Physical Damage						
SA1	Self-administration process model design meetings including but not limited to: scope of claim files (claim, reserves, payments, adjuster notes, subrogation, etc.), identification and definition of custom fields, workflow automation of email notifications, task assignments, and field updates, business rules, subrogation fields and processes, screen layouts, approval process triggered by data conditions and submission for approval/denial of invoice, recommended bill adjustment or subrogation referral, security requirements, correspondence letters, schedule production reports and operational reports approval processes	County and Riskconnect	Week 2	Week 2		A3 - agenda item for A6
SA2	Write Requirements document	Riskconnect	Week 2	Week 3	Milestone	SA1
SA3	Approve Requirements Document	County	Week 3	Week 4	Milestone	SA2
SA4	Build custom fields, data validation rules, record types and screen layouts	Riskconnect	Week 4	Week 15		SA3, H4
SA5	Configure for business rules that execute workflow for email notifications, task assignments and field updates	Riskconnect	Week 4	Week 15		SA3
SA6	Build approval processes and check request output	Riskconnect	Week 4	Week 15		SA3
SA7	Correspondence setup and configuration	Riskconnect	Week 4	Week 15		SA3
SA8	Configure security for users with profiles and sharing model and roles as needed	Riskconnect	Week 4	Week 15		SA3
SA9	Self-administration and Subrogation training for testing	Riskconnect and County	Week 15	Week 16	Milestone	SA4 - SA8 probably web-based training
SA10	County testing of self-administration and subrogation	County	Week 16	Week 17	Milestone	SA9

SA11	Remediation	County and Riskconnect	Week 16	Week 17		Concurrent with SA10
SA12	System Configuration and Design for Self-Administration and Subrogation upon written approval by the County Risk Management	County	Week 18	Week 18		SA11
Litigation Management						
LM1	Business requirements and design meeting for litigation management	County and Riskconnect	Week 1	Week 2		A3 - agenda item for A6
LM2	Write Requirements document	Riskconnect	Week 2	Week 3	Milestone	LM1
LM3	Approve Requirements Document	County	Week 4	Week 4	Milestone	LM2
LM4	Configure litigation management custom fields, data validation rules, screen layouts and workflow for email notifications, task assignments and automatic field updates	Riskconnect	Week 18	Week 23		LM3
LM5	Design and build approval processes	Riskconnect	Week 18	Week 23		LM3
LM6	Expand Correspondence setup for litigation letters	Riskconnect	Week 18	Week 23		LM3
LM7	Update security configuration for litigation management access	Riskconnect	Week 18	Week 23		LM3
LM8	Litigation calendar feature	Riskconnect	Week 18	Week 23		LM3
LM9	Litigation Management training for testing	Riskconnect and County	Week 23	Week 23	Milestone	LM4 - LM8
LM10	County testing of Litigation Management	County	Week 23	Week 25	Milestone	LM9
LM11	Remediation	County and Riskconnect	Week 23	Week 25		Concurrent with LM10
LM12	County Approval for Litigation Management	County	Week 25	Week 25	Milestone	LM11
Data Interface Inbound to Riskconnect from County CAPS+						
CAPS1	Data Generation and Delivery to RK (secure file transfer and documentation to interpret data)	County	Week 4	Week 7	Milestone	A4
CAPS2	Raw Data Staging/Analysis	Riskconnect	Week 6	Week 9		CAPS+1
CAPS3	Mapping/Design	County and Riskconnect	Week 9	Week 10		CAPS+1
CAPS4	Riskconnect Acceptance of CAPS+ data	Riskconnect	Week 11	Week 11	Milestone	CAPS+2 - CAPS+3
CAPS5	Development (includes user interface for resolving unmatched payments)	Riskconnect	Week 23	Week 26		CAPS+4
CAPS6	Riskconnect QA	Riskconnect	Week 26	Week 28		CAPS+5
CAPS7	Remediation	Riskconnect and County	Week 26	Week 28		Concurrent with CAPS+6
CAPS8	County Approval	County	Week 28	Week 28	Milestone	CAPS+7
Data Interface Inbound to Riskconnect - One-Time Conversion County LCMS						

LCMS1	Data Generation and Delivery to RK (secure file transfer and documentation to interpret data)	County	Week 4	Week 5	Milestone	A4
LCMS2	Raw Data Staging/Analysis	Riskconnect	Week 5	Week 6		LCMS1
LCMS3	Mapping/Design	County and Riskconnect	Week 6	Week 9		LCMS1
LCMS4	Riskconnect Acceptance of LCMS data	Riskconnect	Week 9	Week 9	Milestone	LCMS2 - LCMS3
LCMS5	Development	Riskconnect	Week 20	Week 23		LCMS4
LCMS6	Riskconnect QA	Riskconnect	Week 23	Week 25		LCMS5
LCMS7	Remediation	Riskconnect and County	Week 23	Week 25		Concurrent with LCMS6
LCMS8	County Approval	County	Week 26	Week 26	Milestone	LCMS7
Data Interface Inbound to Riskconnect - One-Time Conversion County Historical Reserves						
RES1	Data Generation and Delivery to Riskconnect(secure file transfer and documentation to interpret data)	County	Week 5	Week 7	Milestone	A4
RES2	Raw Data Staging/Analysis	Riskconnect	Week 7	Week 7		RES1
RES3	Mapping/Design	County and Riskconnect	Week 7	Week 8		RES1
RES4	Riskconnect Acceptance of Historical Reserves data	Riskconnect	Week 8	Week 8	Milestone	RES2 - RES3
RES5	Development	Riskconnect	Week 21	Week 23		RES4
RES6	Riskconnect QA	Riskconnect	Week 23	Week 25		RES5
RES7	Remediation	Riskconnect and County	Week 23	Week 25		Concurrent with RES6
RES8	County written acceptance of Data Interface Inbound to Riskconnect including verification of the One-Time conversion of County's historical data reserves	County	Week 26	Week 26		RES7
Data Interface Inbound to Riskconnect - One-Time Conversion County Litigation Log						
LL1	Data Generation and Delivery to RISKCONNECT (secure file transfer and documentation to interpret data)	County	Week 5	Week 6	Milestone	A4
LL2	Raw Data Staging/Analysis	Riskconnect	Week 7	Week 7		LL1
LL3	Mapping/Design	County and Riskconnect	Week 7	Week 8		LL1
LL4	Riskconnect Acceptance of Litigation Log data	Riskconnect	Week 8	Week 8	Milestone	LL2 - LL3
LL5	Development	Riskconnect	Week 25	Week 28		LL4
LL6	Riskconnect QA	Riskconnect	Week 28	Week 30		LL5
LL7	Remediation	Riskconnect and County	Week 28	Week 30		Concurrent with LL6
LL8	County Approval	County	Week 30	Week 30	Payment Milestone #2	LL7
Data Interface Inbound to Riskconnect - One-Time Conversion County Diary						

DY1	Data Generation and Delivery to Riskconnect (secure file transfer and documentation to interpret data)	County	Week 6	Week 7	Milestone	A4
DY2	Raw Data Staging/Analysis	Riskconnect	Week 8	Week 8		DY1
DY3	Mapping/Design	County and Riskconnect	Week 8	Week 9		DY1
DY4	Riskconnect Acceptance of Diary data	Riskconnect	Week 9	Week 9	Milestone	DY2 - DY3
DY5	Development	Riskconnect	Week 25	Week 28		DY4
DY6	Riskconnect QA	Riskconnect	Week 28	Week 30		DY5
DY7	Remediation	Riskconnect and County	Week 28	Week 30		Concurrent with DY6
DY8	County Approval	County	Week 30	Week 30	Payment Milestone #2	DY7
Data Interface Bi-Directional Riskconnect <--> ISO for Claim Query						
ISO1	Format Receipt /Definition	County, Riskconnect and ISO	Week 3	Week 5	Milestone	A 4
ISO2	Mapping/Design	County and Riskconnect	Week 10	Week 11		ISO1
ISO3	Development	Riskconnect	Week 16	Week 19		ISO2
ISO4	Riskconnect QA and Test Files Generation	Riskconnect and ISO	Week 19	Week 23	Milestone	ISO3
ISO5	Remediation	Riskconnect, County and ISO	Week 19	Week 23		Concurrent with ISO4
ISO6	County and Riskconnect Approval	County and Riskconnect	Week 24	Week 24	Milestone	ISO5
Data Interface Bi-Directional Riskconnect <--> ISO CMS						
CMS1	Format Receipt /Definition	County, Riskconnect and ISO	Week 3	Week 5	Milestone	A 4
CMS2	Mapping/Design	County and Riskconnect	Week 11	Week 13		CMS1
CMS3	Development	Riskconnect	Week 19	Week 23		CMS2
CMS4	Riskconnect QA and Test Files Generation	Riskconnect and ISO	Week 24	Week 28	Milestone	CMS3
CMS5	Remediation	Riskconnect, County and ISO	Week 24	Week 28		Concurrent with CMS4
CMS6	County Approval	County	Week 28	Week 28	Milestone	CMS5
Reports and Dashboards						
R1	Report Requirements collection of samples	County and Riskconnect	Week 2	Week 4		A6 (or can be concurrent with A6)
R2	Document report requirements	Riskconnect	Week 5	Week 7	Milestone	R1
R3	Approve written report requirements	County	Week 8	Week 8	Milestone	R2
R4	Reporting Infrastructure and Framework	Riskconnect	Week 8	Week 11		R3, SA4 and likely other specific

						modules
R5	Validate standard reports and dashboards	Riskconnect	Week 15	Week 25	Milestone	R3 and presence of relevant data if such data is part of SOW
R6	Build County reports and dashboards	Riskconnect	Week 15	Week 30		R4 (will be iterative as each major part completes)
R7	QA County reports and dashboards	Riskconnect and County	Week 18	Week 32		R6 (will be iterative as each major part completes)
R8	Remediation	Riskconnect and County	Week 18	Week 32		Concurrent with R7 (will be iterative as each major part completes)
R9	County Approval	County	Week 32	Week 32	Milestone	R8
Training						
T1	Basic system training for any users not included in the training for testing noted in bold above throughout this column	County and Riskconnect	Week 23	Week 26	Milestone	See bold training entries in sections above. Repeated as needed using web-based training or recorded videos when additional users come online
T2	Reports and Dashboards training	County and Riskconnect	Week 23	Week 29	Milestone	T1 See sections above. Introduction to reports and dashboards may be simultaneous with basic system training. Repeated as needed when additional users come online
T3	System Administrator training	County and Riskconnect	Week 24	Week 29	Milestone	T1 - T2 (for Admin users)

Phase 1 Deployments and Overall Completion						
PROD1	County produces for Riskconnect cut-off data for location hierarchy, LCMS, Litigation Log, Diary, Historical Reserves	County	Week 30	Week 30	Milestone	LCMS8, RES8, LL8, DY8
PROD2	Cut-off data files acceptance	Riskconnect	Week 31	Week 31	Milestone	PROD1
PROD3	Load and validate cut-off data	Riskconnect	Week 31	Week 31	Milestone	PROD2
PROD4	Final System Acceptance, Production system on-line and approved in writing by the County	County and Riskconnect	Week 31	Week 31	Milestone	T1 - T3, PROD3, H6, SA12, LM12, CAPS+8
PROD5	Production feeds from CAPS+ to Riskconnect	County and Riskconnect	Week 31	on-going	Milestone	CAPS+8, PROD4
PROD6	Live data transfers to ISO for Claim Query	Riskconnect and ISO	Week 31	on-going	Milestone	ISO6, PROD4
PROD7	Live data transfers to ISO for CMS Reporting	Riskconnect and ISO	Week 31	on-going	Milestone	CMS6, PROD4
PROD8	Schedule and run production reports	Riskconnect	Week 31	on-going	Milestone	R9, PROD4
PROD 9	Go-live settle-in period	Riskconnect and County	Week 31	Week 33	Payment Milestone #3	PROD4
PROD 10	County Implementation Close out	County and Riskconnect	Week 33	Week 33	Milestone	PROD4 - PROD9

Operational Readiness Phase

The purpose of this Phase is to configure, integrate, and test the final application.

Step	Activity Highlights	Deliverable	Responsible
Configuration Riskconnect RCMIS	The purpose of this activity is to complete the configuration work specified in the design phase of the Riskconnect SRCMIS and incident management applications. The County will review system configuration against design documentation.	Location Hierarchy Global System Security Exposure Values Screen design for all modules specified under the RCMIS system design deliverable	Riskconnect
Develop and Implement Data Conversions	The purpose of this activity is to develop and perform the data conversions for all sources. Data conversions will begin once the data is received by Riskconnect. The Riskconnect data conversion specialist will prepare the data conversions, run and validate the data conversions, and perform reconciliation of any financial discrepancies for all data sources.	Data in Riskconnect RCMIS	Riskconnect
Validate Data Conversions	The purpose of this activity is to have the County validate the data conversions.	Data Quality Reports	The County

Claims Admin	Configuration of screens, workflow rules, and security permissions needed for the County to administer claims.	Screen configuration and workflow rules	Riskconnect
Testing Claims Admin Functionality	The County will validate the claims admin workflow.	Testing data entry in claims module	The County
Develop Training Plan	The purpose of this activity is to create an training plan	Training Plan	Riskconnect
Prepare for Production (Integration Testing)	The purpose of this activity is to ensure that the system meets agreed upon specifications and documentation.	Riskconnect RCMIS ready for production	Riskconnect
Conduct Training	The purpose of this activity is to conduct the user training according to the training plan.	User Training	Riskconnect
User Testing of Riskconnect RCMIS	The purpose of this activity is for The County to review system configuration, data conversions, and reports.	User Sign off	The County
Planning for Release of Production System user base	The purpose of this activity is to plan the release of the Riskconnect RCMIS to the County's user community.	Communication plan and support guidelines	Riskconnect

Execute Phase Completion Criteria: The Execute Phase will be considered complete when:

- System design has been completed per the system design specifications
- Data conversions have been completed per the data conversion specifications
- Custom reports have been completed
- The training plan has been delivered to the County
- The County system has been configured per the specifications
 - Riskconnect senior consultant has provided approval that all areas of the Riskconnect RCMIS program are ready to be installed to begin initial testing
- Ongoing support requirements document has been delivered to the County
- The County gives written approval of completion

● The Close Phase

The purpose of the Close Phase is to move the system into production and provide post production and implementation support, in compliance with the implementation strategy.

Step	Activity Highlights	Deliverable	Responsible
Implementation Review	The purpose of this activity review the implementation process and plan for the operation support of Riskconnect RCMIS.	Implementation wrap-up meeting	Riskconnect

Close Phase Completion Criteria: The Close Phase will be considered complete when:

- Riskonnect RCMIS in production
- Implementation Review Meeting has been completed
- County sign-off on all elements of the implementation

ATTACHMENT E

Attachment E Intentionally left blank

ATTACHMENT F

TRAINING AND DOCUMENTATION

CONTRACT MA-017-14010752

1. Riskconnect will provide administrator training to the County administrators.
2. Riskconnect will provide a knowledge transfer plan to insure proper training of County employees.
3. Riskconnect will offer the County end-user training via a live or recorded webinar to meet County's specific training needs.
 - a. Riskconnect will provide instructional videos of specific RCMIS functionality such as using a particular module, and step-by-step instructions on how to use the Proposed Solution.
 - b. Riskconnect shall provide an online help directory and printable user guides and manuals on how to use the Proposed Solution.
 - c. Riskconnect will provide continuous user training on newly released product features and functionality per the training methods listed above.
 - d. Riskconnect will offer multiple training options for staff in technical and specialist areas such as site management, creating templates and workflows.
4. Riskconnect's software knowledge transfer and training will include:
 - a. Customized training guides complete with exercises and County-specific configuration examples. Riskconnect will provide all training materials online and updated by Riskconnect in conjunction with each platform upgrade. Riskconnect will ensure that all County configurations and modifications are included in the system documentation.
 - b. System Administrator Training includes all system setup and configuration tools.
 - c. Riskconnect offers online help. All users have a Help button in upper right-hand corner of all application screens which provides access to online help documentation. In addition, Riskconnect offers customized help on page layouts and fields. Page layouts can be configured to place help and info icons to organization specific fields or provide guidance to users. Field level help allows users to provide help text detailing the purpose and function of any field. In addition, info icons are located next to fields which provide help content related to the field.
5. Other Riskconnect's Training Opportunities
 - a. Riskconnect will provide the County training in the manner in which it will be best received by the users, including, but not limited to video, webinar, and classroom, train the trainer, and tutorials. Riskconnect also features a robust client community that continually assists one another in enhancing the County experience. County training and access to the client community are included in the annual licensing cost.

- b. Additionally, Riskonnect regularly hosts online webinars, which are recorded and available and posted online for convenient viewing. To view an example go to:
http://www.youtube.com/watch?v=oQ_Lp358W7o
 - c. Riskonnect offers training and webinars throughout the year. We additionally offer Riskonnect University, which is a training program available to our clients. Riskonnect University is available via:
<http://www.riskonnect.com/training-support/training-0/riskonnect-university/>
6. Detailed Training Plan for the County

Initial client training consists of 2 full days, delivered onsite. This may be adjusted as needed based on County's needs. We anticipate 1.5 days for all users with an additional .5 day specific to Administrator training. Content of the detailed training plan will be developed by Riskonnect and provided to the County in accordance with the Implementation Plan.

ATTACHMENT G

RISKONNECT SERVICE PERFORMANCE AND ONGOING SUPPORT SERVICES

Contract MA-017-14010752

1. Riskconnect's Hosting Facility

- A. Riskconnect's data center will 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.
- B. Riskconnect's data center facility functions when off the power grid using a back-up generator or other source of electricity.
- C. All County equipment and data hosted at Riskconnect's data center will 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.
- D. Riskconnect will provide infrastructure and support for two (2) environments; one to run a production instance of RCMIS software; and another for the development/test instance of RCMIS software.
- E. The production instance of RCMIS software will include a disaster recovery solution and plan that will enable RCMIS software service delivery to resume as normal within twenty four (24) hours of experiencing a critical system failure or catastrophic event that prevents RCMIS software from functioning properly in accordance with the County Availability requirement.
- F. Riskconnect's disaster recovery services will be tested prior to the implementation of the County's configuration of the Riskconnect Service, and annually thereafter, in accordance with the Contract's disaster recovery requirements.
- G. Riskconnect will cooperate with any County on-site audit or penetration test of Riskconnect managed systems as described in Section 8(h) to this Attachment G.
- H. Upon County's request, Riskconnect will disclose to the County any data security audits [such as SSAE 16 audits] performed within a year of the Contract's Effective Date as well as the results of future such audits. Any issues identified during such audits will be communicated promptly to the County, including the appropriate plan to address or mitigate any issues.

2. Architectural, Performance, Sizing and Capacity Planning Services

Riskconnect will provide system architectural, sizing and capacity planning recommendations that will enable production RCMIS website to operate at optimal performance and within acceptable County Service Levels at all times.

- A. Riskconnect will architect production RCMIS website to meet County performance, security and infrastructure requirements.
- B. Riskconnect will conduct routine architectural, capacity and operational reviews of the County's production RCMIS software environment and, at a minimum annually, recommend and implement architectural improvements to improve RCMIS software performance, Availability, reliability and sustainability in accordance with County minimum performance targets.

3. **IT Service Management**

Riskconnect will manage the RCIMS software and all supporting software and hardware environments using an IT life cycle service management framework that utilizes industry standards and best practices such as those found in BSI 15000, ISO 9000, ISO 17799, ISO 20000, COBIT and ITIL/ITSM.

- A. Riskconnect will perform proactive and reactive operational support tasks that will result in the fulfillment of County RCIMS Service Level requirement performance targets RCIMS Performance and Service Levels.
- B. Riskconnect will perform 24x7x365 Incident logging, troubleshooting, resolution and escalation per Incident Service Level requirements.
- C. Riskconnect will perform routine health checks of the hardware, software and equipment utilized to provide Services to the County. County may also be able to monitor performance of the Riskconnect Service (including latency and uptime availability) by checking the County's node [to be determined during implementation] at trust.salesforce.com.
- D. Riskconnect will perform system changes in accordance with an agreed upon change management and notification process.
- E. Riskconnect will perform routine system maintenance and planned system changes within an agreed upon Maintenance Window or County agreed upon schedule.
- F. Riskconnect will perform and retain backups of all County Data in the Riskconnect Service in accordance with backup requirements as set forth in Section 64 of the Contract.

4. **Other RISKCONNECT SERVICE Maintenance and Support**

Riskconnect will be responsible for providing the County with other software licensing, installation, maintenance and support for all Riskconnect hosted environments (production and test/development). This includes database, middle-ware, web service layers and hardware operating system and required to deliver the RCMIS Services.

- A. Riskconnect will provide all other software licensing, installation, maintenance and support services for each County environment (production and development/test) hosted by Riskconnect.
- B. Riskconnect will provide proactive monitoring of all RCMIS application components to recommend and perform appropriate corrective action when conditions exists that place RCMIS solution and related systems at risk of technical failure, service degradation or a service Outage.
- C. Riskconnect will perform RCIMS application performance tuning as deemed necessary to enable the RCMIS application to perform within specified Service Levels described herein.
- D. Technical Support Availability:
 - 1. The County can communicate with Riskconnect's Service team through phone, email, via your Riskconnect RCMIS through the Riskconnect Request Tab or other functionality inherent in the Riskconnect the Service. These functions ensure complete transparency and prompt responsiveness with Riskconnect client users. Riskconnect support is available to you 24 hours a day, 7 days a week.
 - 2. All support requests, information, and resolution will be tracked in the Riskconnect Request module within the County's configuration of the Riskconnect Service. Riskconnect will provide the County the ability to create requests through direct entry or via e-mail to rkrequest@riskconnect.com. Riskconnect will also accept requests via phone calls.
 - 3. Regardless of entry mechanism, Riskconnect will classify requests by the priority fields as described in Table 2 to Section 7 of this Attachment G.

E. Software Annual Maintenance and Support. Riskconnect will provide annual maintenance in the annual maintenance fees. Annual maintenance includes three

(3) to four (4) platform upgrades every year, which will provide the County new functionality and innovation. Riskconnect will upgrade the County's implementation (which includes standard and County-specific configurations) seamlessly via the

Web with less than five (5) minutes of downtime per upgrade.

F. All Software version updates, system updates and fixes will be provided to the County via the web.

G. Patches / maintenance releases are deployed via the web to the entire Riskconnect client community at once and will support both the standard platform and County-specific configurations.

H. Any changes in scope beyond those Optional Services set forth in Section 10 of Attachment B shall require a Contract amendment.

I. Riskconnect level of maintenance and support after "Go Live" -- The Riskconnect Implementation team will become the County's client service team. Riskconnect support is available to the County 24 hours a day, 7 days a week. The County will be assigned an Account Director, a dedicated account manager with a support staff of data engineers, business analyst, and technical engineers who will comprise County's client service team.

5. RCMIS Application Performance Testing, Monitoring and Reporting

To ensure the Riskconnect Service performs at levels provided in Section 7 to this Attachment G:

- A. Riskconnect will monitor the County User experience using RCMIS application to ensure that the application and its interfaces are performing within County defined performance levels.
- B. Riskconnect will document RCMIS application performance issues and notify County contacts via e-mail when performance levels are below levels in the SLA provided in Section 7 to this Attachment G.
- C. Riskconnect will identify the root cause of performance degradation and take corrective action to resolve issues and promptly bring performance back within acceptable levels; the root cause analysis will be provided to the County within five (5) days of the Incident being reported.
- D. Once the County's configuration of the Riskconnect Service has been implemented, County shall be able to monitor performance of the Riskconnect Service (including latency and uptime availability) by checking the County's node [to be determined during implementation] at trust.salesforce.com.
- E. Riskconnect will perform a system stress test of the RCMIS solution using a mutually agreed upon test script prior to implementation of the RCMIS solution on the production instance as well as through the duration of the Contract as and when major application or module changes are introduced into RCMIS.
 - 1. Riskconnect will initiate web site system stress testing when application changes are applied, or as deemed necessary by the County, to ensure the RCMIS environment remains capable of meeting defined performance levels.
 - 2. Riskconnect will develop reusable RCMIS stress test scripts.
- F. Riskconnect will report the results of the stress test to the County in a mutually agreed upon timeframe. Riskconnect will and initiate appropriate corrective action on production RCMIS instance when stress test results do not meet site performance requirements

6. Security

Riskconnect shall:

- A. Locate all hosted infrastructure behind a firewall in a DMZ, and have a dedicated scheme on a database server allowing access only from the County
- B. Conform all firewall rules to "Best Practices" and Riskconnect must routinely review logs;
- C. Deploy Intrusion Detection and monitor it 24 x 7 x 365
- D. Support the County when it chooses to randomly review Riskconnect's firewall and IDS logs relative to County Data
- E. Securely store passwords with at a minimum of either 256 bit encryption; a cryptographic hash function, or other technology as will be made available in the future
- F. Operate anti-virus software must be running on all computing resources (servers, PC's, etc.) with the most up-to-date signature files;
- G. Communicate any planned software and hardware patch implementations to the County prior to installation
- H. Transmit Count Data using a secure transaction; Riskconnect will use the County's secure FTP solution for bulk file transfers
- I. Encrypt all sessions with 128 bit encryption
- J. Provide access to the RCMIS via a web browser and create individual end User accounts which are unique and support strong, non-repudiation with audit capabilities
- K. Riskconnect will cooperate with any County on-site audit or penetration test of Riskconnect managed systems as described in Section 8(h) to this Attachment G.
- L. Review security and operating practices annually and notify the County of any planned updates in Riskconnect's discretion to procedures to conform to best practices. Comply with all applicable statutes and regulations concerning the privacy and confidentiality of information (GLB, HIPAA, AB1386, etc.);
- M. Provide upon County request a copy of its System Reuse and Mass Storage Decommissioning Policies. Riskconnect must immediately notify the County of any and all Intrusions, Security Violations and/or Incidents as provided in Business Associate Agreement found in Attachment H to Contract. The County reserves the right to participate in any reasonable and consequential investigation at the level of involvement deemed reasonably necessary by the County.

7. Infrastructure And Application Performance and Service Levels

Riskconnect will be responsible for meeting the Riskconnect Service Availability and performance targets and support Service Levels as described herein. Riskconnect will retain the requisite personnel, processes, facilities and infrastructure to ensure County metrics and service requirements are met in accordance with the agreement.

Riskconnect's RCMIS site performance and Service Levels include:

RISKCONNECT SERVICE LEVELS

System Operation Service Levels. Riskconnect shall provide the Riskconnect Service to COUNTY under the Agreement so that all of the quantitative measurements set forth in the first column of Table 1 below (each, a "Metric") satisfy the corresponding specifications set forth in the second column of Table 1 below (each, a "Standard"). If any Metric does not satisfy one or more of its corresponding Standards, then Client will be entitled to receive the corresponding remedy(ies) set forth in the third column of Table 1 (each, a "Remedy"). One (1) Credit = 10% of the **prorated** annual fees - prorated for the Measurement Period (One calendar month). For purposes of the Riskconnect Service availability and levels below, unavailability of the Riskconnect Service shall not include scheduled maintenance, emergency maintenance or any other agreed-to scheduled downtime activity.

Table 1. Service Levels for System Operation

Metric	Standard	Remedy
<u>Availability</u> – Percentage of Measurement Intervals that are not Downtime as measured by trust.salesforce.com.	99.7% + for the period between 7am to 7pm EST, Monday through Friday, of each Measurement Period 99.3% + of each Measurement Period	One Credit for each 0.5 percentage points below Standard
	90.0% + of any Measurement Period	Right of Termination for Deficiency
<u>Latency</u> – Longest round trip time between any two points within the Service Network as measured by trust.salesforce.com. (Excludes client network latency)	3.5 Seconds	One credit for each percentage of the Measurement Period
	5+ seconds for 10% of Measurement Period	Right of Termination for Deficiency
<u>Data Protection</u> – Failure to store all Client Data generated on previous day onto non-volatile memory and contemporaneously record completion	Each occurrence	One Credit
Total Credits accumulated during any Measurement Period	20 Credits	Right of Termination for Deficiency if not corrected by the end of next Measurement Period

Remedial Maintenance Service Levels. Riskonnect shall respond to and resolve problems so as to meet all of the Service Levels in Table 2 below. If Riskonnect does not satisfy one or more of those Service Levels, COUNTY shall be entitled to receive the credits specified below.

Notice of Delayed Resolution. If Riskonnect does not resolve a problem within the Resolution Times listed in Table 2 below, COUNTY shall immediately notify Riskonnect. Riskonnect shall respond immediately with notice that will include: (i) a reasonable explanation for the delay and (ii) a good faith schedule and plan for correction. This notice shall not constitute an excuse or waiver of performance. Riskonnect shall keep County informed of the progress of its efforts to resolve Priority 1 or 2 problems at appropriate intervals or as requested by County.

Table 2. Service Levels for Remedial Maintenance

Problem Priority	Priority Definition	Required Response Time/ Remedy	Required Resolution Time/ Remedy	Required Action/Escalation

<p>Priority 1 (Critical)</p>	<p>A problem that: (i) prevents the System from processing a critical business process or function or materially hinders work or use of the System by a User, (ii) prevents a User from using the System to provide services in compliance with applicable Law, (iii) prevents one or more users from accessing data or putting new data into the System, (iv) causes loss or corruption of data, or (v) leaves the System without a working backup for the System or a User's environment. In addition, Priority 1 problems include any Priority 2 problem that has remained unresolved for a period of 24 hours after Riskconnect learns of the problem.</p>	<p><u>Standard:</u> Immediate (i.e., less than 60 minutes).</p> <p><u>Remedy:</u> 1 Credit: if Response Time exceeds 60 minutes;</p> <p>and for each 60 minute interval thereafter until a response is provided.</p>	<p><u>Standard:</u> 4 consecutive hours for a Workaround.</p> <p><u>Remedy:</u> 1 Credits: if Resolution Time for a Workaround exceeds 8 hours; and for each 4 hour interval thereafter until a Workaround is provided.</p> <p><u>Standard:</u> 12 hours for a fully tested permanent correction.</p> <p><u>Remedy:</u> 1 Credits: if Resolution Time for a permanent correction exceeds 12 hours; and 1 credit for each 4 hour interval thereafter until a permanent correction is provided.</p>	<p>Riskconnect will use all commercially reasonable efforts to resolve each problem as quickly as possible within 1 hour after Riskconnect learns of the problem, or within a shorter timeframe as the parties may otherwise agree. Riskconnect will provide qualified Riskconnect technical support and developer personnel, as needed, to work on the problem exclusively and continuously until it is corrected. If not resolved within 12 hours, Riskconnect's Vice President for Support will be paged and Riskconnect will further escalate its efforts to resolve the problem.</p>
-------------------------------------	---	---	--	---

<p>Priority 2 (Serious)</p>	<p>A problem that affects any process or function that is non-critical but is material to Client's business. A Priority 2 problem may be composed of a collection of problems that would otherwise individually constitute Priority 3 problems, but which, taken as a whole, have the effect of a Priority 2 problem.</p>	<p><u>Standard:</u> Immediate (i.e., less than 2 hours)</p> <p><u>Remedy:</u> 1 Credit: if Response Time exceeds 3 hours; and for each 1 hour interval thereafter until a response is provided.</p>	<p><u>Standard:</u> 8 hours for a Workaround.</p> <p><u>Remedy:</u> 1 Credit: if Resolution Time for a Workaround exceeds 8 hours; and 1 credit for each 8 hour interval thereafter until a Workaround is provided.</p> <p><u>Standard:</u> 24 hours for a fully tested permanent correction.</p> <p><u>Remedy:</u> 1 Credits: if Resolution Time for a permanent correction exceeds 24 hours; and 1 credit for each 8 hour interval thereafter until a permanent correction is provided.</p>	<p>Riskconnect will use all commercially reasonable efforts to resolve each problem as quickly as possible within 8 hours after Riskconnect learns of the problem, or within a shorter timeframe as the parties may otherwise agree. Riskconnect will provide qualified technical support and developer personnel, as needed, to work on the problem exclusively and continuously until it is corrected.</p> <p>If not resolved within 24 hours, Riskconnect's Vice President for Support will be paged and Riskconnect will further escalate its efforts to resolve the problem.</p>
------------------------------------	---	--	---	---

<p>Priority 3 (Moderate)</p>	<p>A problem that affects any process or function that is non-critical to Client's business, but does not qualify as a Priority 1 or a Priority 2 problem.</p>	<p><u>Standard:</u> 48 hours.</p> <p><u>Remedy:</u> 1 Credit: if Response Time exceeds 48 hours; and for each 24 hour interval thereafter until a response is provided.</p>	<p><u>Standard:</u> 48 hours for a Workaround.</p> <p><u>Remedy:</u> 1 Credit: if Resolution Time for a Workaround exceeds 48 hours; and 1 credit for each 24 hour interval thereafter until a Workaround is provided.</p> <p><u>Standard:</u> A fully tested permanent correction as part of Riskconnect's next regularly scheduled release or update.</p> <p><u>Remedy:</u> 1 Credit: if a permanent correction is not provided with Riskconnect's next release or update; and 1 credit for each release or update thereafter until a permanent correction is provided.</p>	<p>Riskconnect will use all commercially reasonable efforts to resolve each Priority 3 problem within 48 hours after Riskconnect learns of the problem, or within a shorter timeframe as the parties may otherwise agree. Riskconnect will provide qualified Riskconnect technical support and developer personnel, as needed, to work on the problem until it is corrected.</p>
-------------------------------------	--	--	---	--

8. Infrastructure Hosting Facility

Riskconnect shall provide RCMIS Services for the County and host County Data in a data center that is secure and protected.

a) Riskconnect shall ensure access, control and physical security that meets these standards:

- 24-hour manned security, including foot patrols and perimeter inspections
- Biometric scanning for access
- Dedicated concrete-walled Data Center rooms
- Computing equipment in access-controlled steel cages
- Video surveillance throughout facility and perimeter
- Building engineered for local seismic, storm, and flood risks
- Tracking of asset removal

b) Riskconnect shall provide environmental controls

- Humidity and temperature control
- Redundant (N+1) cooling system

c) Riskconnect shall ensure consistent and redundant power

- Underground utility power feed
- Redundant (N+1) CPS/UPS systems
- Redundant power distribution units (PDUs)
- Redundant (N+1) diesel generators with on-site diesel fuel storage

d) Riskconnect shall provide a secure and redundant network

- Concrete vaults for fiber entry
- Redundant internal networks
- High bandwidth capacity
 - Perimeter firewalls and edge routers block unused protocols
 - Internal firewalls segregate traffic between the application and database tiers
 - Intrusion detection sensors throughout the internal network report events to a security event management system for logging, alerts, and reports

e) Riskconnect shall provide fire detection and suppression

- VESDA (very early smoke detection apparatus)
- Dual-alarmed, dual-interlock, multi-zone, pre-action dry pipe water-based fire suppression

f) Riskconnect shall provide secure transmission and sessions

- Connection via SSL 3.0/TLS 1.0, using global step-up certificates from VeriSign
- Individual user sessions are identified and re-verified with each transaction, using a unique token created at login

g) In addition to meeting the disaster recovery requirements of the Contract, Riskconnect shall provide the following disaster recovery capabilities

- Real-time replication to disk at each data center, and near real-time data replication between the production data center and the disaster recovery center
- Data will be transmitted across encrypted links
- Routine disaster recovery tests to verify projected recovery times and the integrity of the County's Data

h) Riskconnect's penetration testing and remediation process

County shall be responsible for the cost and any scheduling of desired third-party penetration testing prior to Go-Live and Riskconnect shall reasonably accommodate any such testing. Riskconnect shall implement reasonable remedial actions that result from any such testing.

i) Infrastructure sizing and capacity planning services at Riskconnect's hosting facility:

The multi-tenant design of the platform ensures that as the user base and transaction volume increases, the platform adjusts to meet the demands. Salesforce.com's infrastructure design can scale both vertically and horizontally due to its unique pod architecture. A pod is a set of industry standard resources (high-performance database, Web Application, Search, Email, Storage, Backup Servers, Load Balancers, etc.) that work together to serve the needs of a limited collection of organizations and applications. To prevent demand overload of any one pod's resources, Salesforce.com provisions a new pod when existing pods are at or nearing predefined capacity thresholds.

j) Change Management Procedures

Change Request	Procedure
STEP 1	Each Change Request is forwarded to Riskconnect Professional Services by the Client's project manager.
STEP 2	Riskconnect assesses the impact of each Change Request on the project as defined in the existing Statement of Work and may make suggestions and/or modifications to the Change Request.
STEP 3	Client's project manager may approve, reject, or further modify Riskconnect's suggestions and/or modifications.
STEP 4	Upon approval and mutually agreed upon terms, Riskconnect will incorporate Change Request into the project schedule and perform the required work

k) Assumptions

- Riskconnect will manage all Change Requests within the integrated Riskconnect Project Management system.
- Potential impact on the existing deliverable schedules (timelines), and potential changes (both intentional and unintentional) to other components, modules, features, reports and other system functionality will be assessed. Multiple impact assessments will be made as required until final approval is completed.

l) Change Request Response Time

- Change Requests include reports, feature enhancements, user setup, and other functionality you might request. This is not to be confused with system performance and system availability issues

Work Effort	Estimate
LOW	1 - 3 business days to complete
MEDIUM	3 - 7 business days to complete
HIGH	> 7 business days to complete

The estimated values listed above apply to the majority of change requests. However, due to potentially complex reports and other change requests, some change requests may require additional time and/or fees. These change requests will be scoped and approved on an as needed basis by both Parties.

ATTACHMENT H

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.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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 Section 2.3 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.

7. 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 County of Orange

Exhibit I

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 performance 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 County of Orange

Exhibit I

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 Riskonnect determines that returning or destroying the PHI is not feasible, Riskonnect 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, Riskonnect 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 Riskonnect maintains such PHI.

(c) The obligations of this Attachment H shall survive the termination of this Contract.

Attachment I

RISKONNECT PRIVACY STATEMENT

Riskconnect, Inc. (“Riskconnect”, “We”, or “Us”) is committed to protecting the privacy of individuals who visit Riskconnect’s web sites (“Visitors”), individuals who register to use the Services as defined below (“Customers”), and individuals who register to attend Riskconnect’s corporate events (“Attendees”). This Privacy Statement describes Riskconnect’s privacy practices in relation to the use of Riskconnect’s web sites and the related applications and services offered by Riskconnect (the “Services”). This Privacy Statement and associated practices are intended to demonstrate Riskconnect’s commitment to transparency, accountability, and choice regarding the collection and use of your personal information.

Riskconnect also abides by the U.S.-EU Safe Harbor Framework and the U.S.-Swiss Safe Harbor Framework as set forth by the U.S. Department of Commerce and the European Union (“EU”) and Switzerland (collectively referred to as the “Safe Harbor Frameworks”). Riskconnect has certified that it adheres to the Safe Harbor Principles. For more information on the Safe Harbor Frameworks and Safe Harbor Principles, and to view the scope of Riskconnect's certification, please visit <http://www.export.gov/safeharbor/>.

As part of our participation in these Safe Harbor Frameworks, Riskconnect has agreed to dispute resolution by the EU Data Protection Authorities (“EU DPAs”) to serve as an independent recourse mechanism (“IRM”) for dispute resolution arising from collection, use, and retention of personal information transferred from EU member countries to Riskconnect. In choosing the EU DPAs to serve as an IRM for dispute resolution, Riskconnect has remitted the necessary annual fee to the United States Council for International Business (“USCIB”) who acts as a trusted third party on behalf of the EU DPAs with regards to disputes relating to Riskconnect’s compliance with the Safe Harbor Frameworks.

If you have any questions or complaints regarding our compliance with the U.S.-EU Safe Harbor Framework, please see Section 12 (Enforcement) below.

1. WEB SITE COVERED & LINKS TO OTHER SITES

This Privacy Statement covers the information practices of the web sites that link to this Privacy Statement, including <http://www.riskconnect.com>, <http://bi.riskconnect.com>, and <ftp.riskconnect.com>.

For your convenience, Riskconnect may provide links to other web sites and web pages that We do not control. Riskconnect encourages you to review the privacy statements of other web sites to understand their information practices and terms of use.

2. INFORMATION COLLECTED

When expressing an interest in obtaining additional information about the Services or registering to use the Services, We require you to provide us with personal contact information, such as name, company name, address, phone number, and email address (“Required Contact Information”). When purchasing the Services, Riskconnect may require you to provide financial qualification and billing information, such as billing name and

address, credit card number, and the number of employees within the organization that will be using the Services (“Billing Information”). Riskonnect may also ask you to provide additional information, such as company annual revenues, number of employees, or industry (“Optional Information”). Required Contact Information, Billing Information, and Optional Information about Customers are referred to collectively as “Data About Riskonnect Customers”, or in the case of Attendees, “Data About Riskonnect Attendees”.

As you navigate Riskonnect’s web sites, Riskonnect may also collect information through the use of commonly-used information-gathering tools, such as cookies and web beacons (“Web Site Navigational Information”). Web Site Navigational Information includes standard information from your Web browser (such as browser type and browser language), your Internet Protocol (“IP”) address, and the actions you take on Riskonnect’s web sites (such as the web pages viewed and the links clicked). Additional information about the collection of Web Site Navigational Information by Riskonnect can be viewed in Section 4 of this Privacy Statement.

With respect to employees and non-employee personnel of Riskonnect, on occasion, transfers personnel data to the United States in connection with the efficient management and operation of Riskonnect, enabling all Riskonnect personnel to communicate with one another and work together, human resources and benefits administration, and safety and security processes. Riskonnect may also transfer employee and non-employee personnel data to an agent of Riskonnect in connection with the above purposes, such as a payroll provider, benefits provider or background-screening provider. Personnel data may also be processed and transferred to the United States in connection with collection and discovery requests in the context of litigation or government investigations, and in such context it may be made available to adverse parties in litigation or governmental entities.

3. USE OF INFORMATION COLLECTED

Riskonnect uses Data About Riskonnect Customers to perform the services requested. For example, if you fill out a “Contact Me” Web form, Riskonnect will use the information provided to contact you about your interest in the Services.

Riskonnect also uses Data About Riskonnect Attendees to plan and host corporate events in which event attendees may participate and to populate online profiles for Attendees on Riskonnect’s web sites. Additional information on Riskonnect’s privacy practices with respect to Data About Riskonnect Attendees may be found in additional privacy statements on the event web sites, as the case may be.

Riskonnect may also use Data About Riskonnect Customers and Data About Riskonnect Attendees for marketing purposes. For example, Riskonnect may use information you provide to contact you to further discuss your interest in the Services and to send you information regarding Riskonnect, its affiliates, and its partners, such as information about promotions or events.

Riskonnect uses credit card information solely to check the financial qualifications and collect payment from prospective Customers and Attendees.

Riskconnect uses Web Site Navigational Information to operate and improve Riskconnect's web sites. Riskconnect may also use Web Site Navigational Information alone or in combination with Data About Riskconnect Customers and Data About Riskconnect Attendees to provide personalized information about Riskconnect.

4. WEB SITE NAVIGATIONAL INFORMATION

As stated previously, Riskconnect uses commonly-used information-gathering tools, such as cookies and Web beacons, to collect information as you navigate the Company's Web sites ("Web Site Navigational Information"). This section describes the types of Web Site Navigational Information used on Riskconnect's web sites and how this information may be used.

4.1 Cookies. Riskconnect uses cookies to provide additional functionality to the website and to help Us analyze site usage more accurately. When you visit one of Riskconnect's web sites, Riskconnect's servers send a cookie to your computer. Standing alone, cookies do not personally identify you; they merely recognize your web browser. Unless you choose to identify yourself to Riskconnect, either by responding to a promotional offer, opening an account, or filling out a web form, you remain anonymous to Riskconnect.

Riskconnect uses cookies that are session-based and persistent-based. Session cookies exist only during one session. They disappear from your computer when you close your browser software or turn off your computer. Persistent cookies remain on your computer after you close your browser or turn off your computer. Please note that if you disable your web browser's ability to accept cookies, you will be able to navigate Riskconnect's web sites, but you will not be able to successfully use the Services.

4.2 Web Beacons. Riskconnect uses web beacons alone or in conjunction with cookies to compile information about Customers and Visitors' usage of Riskconnect's web sites and interaction with emails from Riskconnect. Web beacons are clear electronic images that can recognize certain types of information on your computer, such as cookies, when you viewed a particular web site tied to the web beacon, and a description of a web site tied to the web beacon. For example, Riskconnect may place web beacons in marketing emails that notify Riskconnect when you click on a link in the email that directs you to one of Riskconnect's web sites. Riskconnect uses web beacons to operate and improve Riskconnect's web sites and email communications.

4.3 IP Addresses. When you visit Riskconnect's web sites, Riskconnect collects your Internet Protocol ("IP") addresses to track and aggregate non-personal information. For example, Riskconnect uses IP addresses to monitor the regions from which Customers and Visitors navigate Riskconnect's web sites.

Riskconnect also collects IP addresses from Customers when they log into the Services as part of Riskconnect's "Identity Confirmation" and "IP Range Restrictions" security features.

5. SHARING OF INFORMATION COLLECTED

5.1 Service Providers. Riskconnect may share Data About Riskconnect Customers and Data About Riskconnect Attendees with Riskconnect's contracted service providers so that these service providers can provide services on Riskconnect's behalf. Riskconnect may also share Data About Riskconnect Customers with Riskconnect's service providers to ensure the quality of information provided. Unless described in this Privacy

Statement, Riskonnect does not share, sell, rent, or trade any information with third parties for their promotional purposes.

5.2 Business Partners. From time to time, Riskonnect may partner with other companies to jointly offer products or services. If you purchase or specifically express interest in a jointly-offered product or service from Riskonnect, We may share Data About Riskonnect Customers collected in connection with your purchase or expression of interest with our joint promotion partner(s). Riskonnect does not control our business partners' use of the Data About Riskonnect Customers we collect, and their use of the information will be in accordance with their own privacy policies. If you do not wish for your information to be shared in this manner, you may opt not to purchase or specifically express interest in a jointly offered product or service.

Riskonnect does not share Data About Riskonnect Attendees with business partners unless: (1) you specifically opt in to such sharing via an event registration form or (2) you register to attend a Riskonnect corporate event, including webinars. If you do not wish for your information to be shared in this manner, you may choose not to opt in via event registration forms and elect not to have your badge scanned at Riskonnect events. If you choose to share your information with business partners in the manners described above, your information will be subject to the business partners' respective privacy statements.

5.3 Billing. Riskonnect uses a third-party service provider to manage credit card processing. This service provider is not permitted to store, retain, or use Billing Information except for the sole purpose of credit card processing on Riskonnect's behalf.

5.4 Compelled Disclosure. Riskonnect reserves the right to use or disclose information provided if required by law or if Riskonnect reasonably believes that use or disclosure is necessary to protect Riskonnect's rights and/or to comply with a judicial proceeding, court order, or legal process.

6. INTERNATIONAL TRANSFER OF INFORMATION COLLECTED

To facilitate Riskonnect's global operations, Riskonnect may transfer and access Data About Riskonnect Customers and Data About Riskonnect Attendees from around the world, including the United States. This Privacy Statement shall apply even if Riskonnect transfers Data About Riskonnect Customers or Data About Riskonnect Attendees to other countries.

7. COMMUNICATIONS PREFERENCES

Riskonnect offers Visitors, Customers, and Attendees who provide contact information a means to choose how Riskonnect uses the information provided. You may manage your receipt of marketing and non-transactional communications by clicking on the "unsubscribe" link located on the bottom of Riskonnect's marketing emails. Additionally, you may send a request specifying your communications preferences to info@riskonnect.com. Customers cannot opt out of receiving transactional emails related to their account with Riskonnect or the Services.

8. CUSTOMER DATA

Riskconnect Customers may electronically submit data or information to the Services for hosting and processing purposes (“Customer Data”). Riskconnect will not review, share, distribute, or reference any such Customer Data except as provided in a Master Subscription Agreement (or comparable agreement with Riskconnect), or as may be required by law. In accordance with a Master Subscription Agreement (or comparable agreement with Riskconnect), We may access Customer Data only for the purpose of: providing the Services (including with our contracted service providers as further described in Section 5.1 hereto); preventing or addressing service or technical problems; at a Customer’s request in connection with customer support matters; or as may be required by law.

9. SECURITY

Riskconnect uses robust security measures to protect Customer Data from unauthorized access, maintain data accuracy, and help ensure the appropriate use of Customer Data. When the Services are accessed using Internet Explorer version 5.0 or later, Firefox version 20.0 or later, Chrome version 24.0 or later, Safari version 5.0 or later, Secure Socket Layer (“SSL”) technology protects Customer Data using both server authentication and data encryption. These technologies help ensure that Customer Data is safe, secure, and only available to the Customer to whom the information belongs and those to whom the Customer has granted access. Riskconnect also implements an advanced security method based on dynamic data and encoded session identifications, and Riskconnect hosts its web sites in a secure server environment that uses firewalls, intrusion detection systems, and other advanced technology to prevent interference or access from outside intruders. Riskconnect also offers enhanced security features within the Services that permit Customers to configure security settings to the level they deem necessary. Customers are responsible for maintaining the security and confidentiality of their Riskconnect usernames and passwords.

Because Riskconnect uses the Services to maintain Data About Riskconnect Customers and Data About Riskconnect Attendees, this information, which is stored in the Services, is secured in the same manner as described above for Customer Data.

10. CORRECTING AND UPDATING YOUR INFORMATION

Riskconnect shall allow you access to your personal Data and allow you to correct, amend or delete inaccurate information, except where the rights of persons other than you would be violated. Any requests We receive by email or webform to access, change, or delete your information will be completed within 30 days. Normally, Customers may update or change their registration information by editing their user profiles or organization records at the appropriate Riskconnect website. Normally, Attendees may update or change their registration information after logging into appropriate Riskconnect website for the given Riskconnect corporate event.

11. CHANGES TO THIS PRIVACY STATEMENT

Riskconnect reserves the right to change this Privacy Statement. Riskconnect will provide notification of the material changes to this Privacy Statement through Riskconnect’s web sites at least thirty (30) business days prior to the change taking effect.

12. ENFORCEMENT

Riskconnect uses a self-assessment approach to assure compliance with this Privacy Statement and periodically verifies that this Privacy Statement is accurate, comprehensive for the information intended to be covered, prominently displayed, completely implemented and accessible and in conformity with the Safe Harbor Frameworks.

If you have any questions or complaints regarding our compliance with the Safe Harbor Frameworks, please contact us. Riskconnect has a designated Director of Technical Operations who oversees and is accountable for the security of Data on Riskconnect's web sites. If a complaint or dispute cannot be resolved through our internal process, Riskconnect agrees to dispute resolution by the EU Data Protection Authorities (EU DPAs) to serve as an independent recourse mechanism (IRM) for dispute resolution.

13. CONTACTING US

Questions regarding this Privacy Statement or the information practices of Riskconnect's web sites should be addressed to Riskconnect's Director of Technical Operations by emailing webmaster@riskconnect.com, or by mailing Riskconnect at 1701 Barrett Lakes Blvd., Suite 500, Kennesaw, GA 30144 USA.

ATTACHMENT J

PLATFORM CONTINUITY TERMS TO THE SFDC PLATFORM SOLUTION RESELLER AGREEMENT WITH RISKCONNECT

As part of an amendment to Riskconnect’s Platform Solution Reseller Agreement with Salesforce.com, Inc. (“SFDC”), SFDC has agreed to the following provision as it relates to Riskconnect’s agreements with its customers, including COUNTY (herein “You” or “Your”):

“Platform Continuity. In the event that SFDC terminates the SFDC Reseller Agreement because Reseller has become the subject of a petition in bankruptcy or any other proceeding relating to insolvency, receivership, liquidation or assignment for the benefit of creditors or Reseller ceases business in the ordinary course (any of which would be an “End of Operations Event” or “EOE” for Reseller), SFDC will continue to make the Platform available to You and SFDC will take no self-initiated steps to (a) remove the Reseller Application from SFDC’s systems or (b) block Your access to the Reseller Application via the Platform for the remainder of Your current order term with Reseller (the “Transition Period”), provided that: (i) You pay to SFDC in advance all fees owed to SFDC with respect to the Platform pursuant to a separate order between You and SFDC; (ii) You remain in compliance with this SFDC Service Agreement; (iii) You are legally entitled to continued access to and use of the Reseller Application in combination with the Platform after an EOE through a written agreement with Reseller or its successor in interest in anticipation of or as a consequence of any EOE; and (iv) there are no legal impediments to SFDC continuing to host the Reseller Application (as reasonably determined by SFDC). Notwithstanding SFDC’s continued provision of the Platform, You understand and acknowledge that SFDC shall not be responsible for providing (other than hosting “as is” subject to the above conditions), updating, maintaining or supporting the Reseller Application during the Transition Period. For the purposes of this section, “SFDC Reseller Agreement” means Reseller’s agreement with SFDC pursuant to which Reseller is providing the Platform as part of the Reseller Application to You, and “Platform” means SFDC’s web-based on-demand platform for developing and operating on-demand applications.”

ATTACHMENT K

County’s User Provisioning Policy

OC-SEC-POL-003 – User Provisioning Policy

Policy Owner:	CISO	Effective Date:	09/01/11
----------------------	------	------------------------	----------

Prepared By:	CEO/IT	Version No.:	1.0
Approved By:	CEO	Publication Date:	PENDING
Approval Date:	PENDING	Next Review:	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.

Term	Definition
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
Agcy -SEC-PRO-003	Agency User Provisioning Procedure	Agency

- Revision History**

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

- Approvals**

Date	Approver Name	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 L

DATA CLASSIFICATION POLICY

Policy Area	IT Policy Library
Approved Date	December 31, 2012
Approved By	CISO
Effective Date	TBD
Current Version	1.0

• I. 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.

• II. 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.

• III. SCOPE

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

• IV. POLICY

Data shall be classified as listed below.

Public - Information intended or required for public release. Information can only be declared Public by an authorized Data Owners 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.

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

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

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.

• V. ENFORCEMENT

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

• VI. DISTRIBUTION

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

Policy History

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