REGIONAL COOPERATIVE AGREEMENT (RCA)
CONTRACT NUMBER RCA-017-25010065
BETWEEN
COUNTY OF ORANGE/COUNTY PROCUREMENT OFFICE
AND
CARAHSOFT TECHNOLOGY CORP
FOR
ON-LINE MARKETPLACE FOR CLOUD SERVICES AND SOFTWARE

This Contract RCA-017-25010065 for On-Line Marketplace for Cloud Services and Software (Contract) is made and entered into as of the date fully executed by and between the County of Orange, a political subdivision of the State of California ("County"), and Carahsoft Technology Corp, a Corporation in Maryland (Contractor), with County and Contractor sometimes referred to as Party or collectively as Parties.

ATTACHMENTS

This Contract is comprised of this document and the following Attachments, which are attached hereto and incorporated by reference into this Contract:

Attachment A – Scope of Work Attachment
B – Payment and Compensation
Attachment C – Information Technology Security Guidelines
Attachment D – Business Associate Contract

RECITALS

WHEREAS, Contractor and County are entering into this Contract for On-Line Marketplace for Cloud Services and Software under a usage Contract; and,

WHEREAS, County solicited Contract for On-Line Marketplace for Cloud Services and Software as set forth herein, and Contractor represented that it is qualified to provide On-Line Marketplace for Cloud Services and Software to the County as further set forth here; and,

WHEREAS, Contractor agrees to provide On-Line Marketplace for Cloud Services and Software to the County as further set forth in the Scope of Work, attached hereto as Attachment A; and,

WHEREAS, County agrees to pay Contractor based on the schedule of fees set forth in Payment/Compensation, attached hereto as Attachment B; and,

NOW, THEREFORE, the Parties mutually agree as follows:

ARTICLES

GENERAL TERMS AND CONDITIONS

1. 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. 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 adjudication to another county.

2. Entire Contract:

This Contract contains the entire Contract between the parties with respect to the matters herein, and there are no restrictions, promises, warranties or undertakings other than those set forth herein or referred to herein. No exceptions, alternatives, substitutes or revisions are valid or binding on County unless authorized by County in writing. Electronic acceptance of any additional terms, conditions or supplemental Contracts by any County employee or agent, including but not limited to installers of software, shall not be valid or binding on County unless accepted in writing by County's Purchasing Agent or designee.

3. Amendments:

No alteration or variation of the terms of this Contract shall be valid unless made in writing and signed by the parties; no oral understanding or agreement not incorporated herein shall be binding on either of the parties; and no exceptions, alternatives, substitutes or revisions are valid or binding on County unless authorized by County in writing.

4. Taxes:

Unless otherwise provided herein or by law, price quoted does not include California state sales or use tax. Out-of-state Contractors shall indicate California Board of Equalization permit number and sales permit number on invoices, if California sales tax is added and collectable. If no permit numbers are shown, sales tax will be deducted from payment. The Auditor-Controller will then pay use tax directly to the State of California in lieu of payment of sales tax to Contractor.

5. Delivery:

Time of delivery of commodities and services is of the essence in this Contract. County reserves the right to refuse any commodities and services and to cancel all or any part of the commodities not conforming to applicable specifications, drawings, samples or descriptions or services that do not conform to the prescribed scope of work. Acceptance of any part of the order for commodities shall not bind County to accept future shipments nor deprive it of the right to return commodities already accepted at Contractor's expense. Over shipments and under shipments of commodities shall be only as agreed to in writing by County. Delivery shall not be deemed to be complete until all commodities or services have actually been received and accepted in writing by County.

6. Acceptance Payment:

Unless otherwise agreed to in writing by County, 1) acceptance shall not be deemed complete unless in writing and until all the commodities/services have actually been received, inspected, and tested to the satisfaction of County, and 2) payment shall be made in arrears after satisfactory acceptance.

7. Warranty:

Contractor expressly warrants that the commodities covered by this Contract are 1) free of liens or encumbrances, 2) merchantable and good for the ordinary purposes for which they are used, and 3) fit for the particular purpose for which they are intended. Acceptance of this order shall constitute an agreement

upon Contractor's part to indemnify, defend and hold County and its indemnities as identified in the Insurance and Indemnification section, and as more fully described in the Insurance and Indemnification section harmless from liability, loss, damage and expense, including reasonable counsel fees, incurred or sustained by County by reason of the failure of the goods/services to conform to such warranties, faulty work performance, negligent or unlawful acts, and non-compliance with any applicable state or federal codes, ordinances, orders, or statutes, including the Occupational Safety and Health Act (OSHA) and the California Industrial Safety Act. Such remedies shall be in addition to any other remedies provided by law.

8. Patent/Copyright Materials/Proprietary Infringement:

Unless otherwise expressly provided in this Contract, Contractor shall be solely responsible for clearing the right to use any patented or copyrighted materials in the performance of this Contract. Contractor warrants that any software as modified through services provided hereunder will not infringe upon or violate any patent, proprietary right, or trade secret right of any third party. Contractor agrees that, in accordance with the more specific requirement contained in the Insurance and Indemnification section, 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, costs and expenses but not including attorney's fees.

9. Assignment:

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 by Contractor without the express written consent of County. Any attempt by Contractor to assign 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.

10. Non-Discrimination:

In the performance of this Contract, Contractor agrees that it will 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. Contractor acknowledges that a violation of this provision shall subject Contractor to penalties pursuant to Section 1741 of the California Labor Code.

11. Termination:

In addition to any other remedies or rights it may have by law, County has the right to immediately terminate this Contract without penalty for cause or after 30 days' written notice without cause, unless otherwise specified. Cause shall be defined as any material breach of contract, any misrepresentation or fraud on the part of Contractor. Exercise by County of its right to terminate Contract shall relieve County of all further obligation.

12. 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.

13. Independent Contractor:

Contractor shall be considered an independent contractor and neither Contractor, its employees, nor anyone working under Contractor shall be considered an agent or an employee of County. Neither Contractor, its employees nor anyone working under Contractor shall qualify for workers' compensation or other fringe benefits of any kind through County.

14. Performance Warranty:

Contractor shall warrant all work under this Contract, taking necessary steps and precautions to perform the work to County's satisfaction**.** Contractor shall be responsible for the professional quality, technical assurance, timely completion and coordination of all documentation and other commodities/services furnished by Contractor under this Contract. Contractor shall perform all work diligently, carefully, and in a good and workmanlike manner; shall furnish all necessary labor, supervision, machinery, equipment, materials, and supplies, 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 work. If permitted to subcontract, Contractor shall be fully responsible for all work performed by subcontractors.

15. Changes:

Contractor shall make no changes in the work or perform any additional work without County's specific written approval.

16. Change of Ownership/Name, Litigation Status, Conflicts with County Interests:

Contractor agrees that if there is a change or transfer in ownership of Contractor's business prior to completion of this Contract, and County agrees to an assignment of Contract, the new owners shall be required under the terms of sale or other instruments of transfer to assume Contractor's duties and obligations contained in this Contract and complete them to the satisfaction of County.

County reserves the right to immediately terminate Contract in the event County determines that the assignee is not qualified or is otherwise unacceptable to County for the provision of services under Contract.

In addition, Contractor has the duty to notify County in writing of any change in Contractor's status with respect to name changes that do not require an assignment of Contract. Contractor is also obligated to notify County in writing if Contractor becomes a party to any litigation against County, or a party to litigation that may reasonably affect Contractor's performance under Contract, as well as any potential conflicts of interest between Contractor and County that may arise prior to or during the period of Contract performance. While Contractor will be required to provide this information without prompting from County any time there is a change in Contractor's name, conflict of interest or litigation status, Contractor must also provide an update to County of its status in these areas whenever requested by County.

Contractor shall exercise reasonable care and diligence to prevent any actions or conditions that could result in a conflict with County interests. In addition to Contractor, this obligation shall apply to Contractor's employees, agents, and subcontractors associated with the provision of goods and services provided under

this Contract. Contractor's efforts shall include, but not be limited to establishing rules and procedures preventing its employees, agents, and subcontractors from providing or offering gifts, entertainment, payments, loans or other considerations which could be deemed to influence or appear to influence County staff or elected officers in the performance of their duties.

17. Force Majeure:

Contractor shall not be assessed with liquidated damages or unsatisfactory performance penalties during any delay beyond the time named for the performance of this Contract caused by any act of God, war, civil disorder, employment strike or other cause beyond its reasonable control, provided Contractor gives written notice of the cause of the delay to County within 36 hours of the start of the delay and Contractor avails himself of any available remedies.

18. Confidentiality:

Contractor 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 Contractor and Contractor's staff, agents and employees.

19. Compliance with Laws:

Contractor represents and warrants that services to be provided under this Contract shall fully comply, at Contractor'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. Contractor acknowledges that County is relying on Contractor to ensure such compliance, and pursuant to the requirements of the Insurance and Indemnification section, Contractor 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.

Contractor shall remain in compliance and in good standing, maintaining current and active business entity and/or nonprofit registration status, with all applicable federal, state and local registration requirements at the time of execution of the contract through the duration of the term of the Contract, and shall provide annual confirmation of current and active status to County through the term of the Contract.

20. Freight:

Prior to County's express acceptance of delivery of products. Contractor assumes full responsibility for all transportation, transportation scheduling, packing, handling, insurance, and other services associated with delivery of all products deemed necessary under Contract.

21. Severability:

If any term, covenant, condition or provision of this Contract is held by a court of competent jurisdiction to be invalid, void, or unenforceable, the remainder of the provisions hereof shall remain in full force and effect and shall in no way be affected, impaired or invalidated thereby.

22. Attorney Fees:

In any action or proceeding to enforce or interpret any provision of this Contract, each party shall bear their own attorney's fees, costs and expenses.

23. 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 had 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 or 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 effect the purpose of the parties and this Contract.

24. Employee Eligibility Verification:

Contractor warrants that it fully complies with all Federal and State statutes and regulations regarding the employment of aliens 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. Contractor 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. Contractor shall retain all such documentation for all covered employees for the period prescribed by the law. Contractor shall indemnify, defend with counsel approved in writing by County, and hold harmless, County, its agents, officers, and employees from employer sanctions and any other liability which may be assessed against Contractor or 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.

25. Audits/Inspections:

Contractor agrees to permit County's Auditor-Controller or the Auditor-Controller's authorized representative (including auditors from a private auditing firm hired by 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 Contractor for the purpose of auditing or inspecting any aspect of performance under this Contract. The inspection and/or audit will be confined to those matters connected with the performance of Contract including, but not limited to, the costs of administering Contract. County will provide reasonable notice of such an audit or inspection.

County reserves the right to audit and verify Contractor's records before final payment is made.

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

Should Contractor cease to exist as a legal entity, Contractor's records pertaining to this Contract shall be

forwarded to County's project manager.

26. Contingency of Funds:

Contractor acknowledges that funding or portions of funding for this Contract may be contingent upon state budget approval; receipt of funds from, and/or obligation of funds by, the state of California to County; and inclusion of sufficient funding for the services hereunder in the budget approved by County's Board of Supervisors for each fiscal year covered by this Contract. If such approval, funding or appropriations are not forthcoming, or are otherwise limited, County may immediately terminate or modify this Contract without penalty.

27. Expenditure Limit:

Contractor shall notify County of Orange assigned Deputy Purchasing Agent in writing when the expenditures against Contract reach 75 percent of the dollar limit on Contract. County will not be responsible for any expenditure overruns and will not pay for work exceeding the dollar limit on Contract unless a change order to cover those costs has been issued.

INDEMNIFICATION AND INSURANCE PROVISIONS

1. Indemnification

Contractor agrees to indemnify, defend with counsel approved in writing by County, and hold County, its elected and appointed officials, officers, employees, agents and those special districts and agencies which County's Board of Supervisors acts as the governing Board ("County Indemnitees") harmless from any claims, demands or liability of any kind or nature, including but not limited to personal injury or property damage, arising from or related to the services, products or other performance provided by Contractor pursuant to this Contract. If judgment is entered against Contractor and County by a court of competent jurisdiction because of the concurrent active negligence of County or County Indemnitees, Contractor and County agree that liability will be apportioned as determined by the court. Neither Party shall request a jury apportionment. Notwithstanding anything stated above, nothing contained herein shall relieve Contractor of any insurance requirements of obligations created elsewhere in this Contract.

2. General Insurance Requirements

Prior to the provision of services under this Contract, the Contractor agrees to carry all required insurance at Contractor's expense, including all endorsements required herein, necessary to satisfy the County that the insurance provisions of this Contract have been complied with. Contractor agrees to keep such insurance coverage current, provide Certificates of Insurance, and endorsements to the County during the entire term of this Contract.

Contractor shall ensure that all subcontractors performing work on behalf of Contractor pursuant to this Contract shall be covered under Contractor's insurance as an Additional Insured or maintain insurance subject to the same terms and conditions as set forth herein for Contractor. Contractor shall not allow subcontractors to work if subcontractors have less than the level of coverage required by County from Contractor under this Contract. It is the obligation of Contractor to provide notice of the insurance requirements to every subcontractor and to receive proof of insurance prior to allowing any subcontractor to begin work. Such proof of insurance must be maintained by Contractor through the entirety of this Contract for inspection by County representative(s) at any reasonable time.

All self-insured retentions (SIR)'s shall be clearly stated on the Certificate of Insurance. Any SIR in excess of Fifty Thousand Dollars $50,000 shall specifically be approved by the County's Risk Manager, or designee. The County reserves the right to require current audited financial reports from Contractor. If Contractor is self-insured, Contractor will indemnify the County for any and all claims resulting or arising from Contractor's services in accordance with the indemnity provision stated in this contract.

If the Contractor fails to maintain insurance acceptable to the County for the full term of this Contract, the County may terminate this Contract.

Qualified Insurer

The policy or policies of insurance must be issued by an insurer with a minimum rating of A- (Secure A.M. Best's Rating) and VIII (Financial Size Category as determined by the most current edition of the **Best's Key Rating Guide/Property-Casualty/United States or ambest.com).** It is preferred, but not mandatory, that the insurer be licensed to do business in the state of California (California Admitted Carrier).

If the insurance carrier does not have an A.M. Best Rating of A-/VIII, the 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 the Contractor shall provide the minimum limits and coverage as set forth below.

Increased insurance limits may be satisfied with Excess/Umbrella policies. Excess/Umbrella policies when required must provide Follow Form coverage.

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

Contractor shall provide thirty (30) days prior written notice to the County of any policy cancellation or non-renewal and ten (10) days prior written notice where cancellation is due to non-payment of premium and provide a copy of the cancellation notice to County. Failure to provide written notice of cancellation may constitute a material breach of the Contract, upon which the County may suspend or terminate this Contract.

Insurance certificates should be forwarded to the agency/department address listed on the solicitation.

If the Contractor fails to provide the insurance certificates and endorsements within seven (7) days of notification by CEO/Purchasing or the agency/department purchasing division, award may be made to the next qualified vendor.

County expressly retains the right to require Contractor to increase or decrease insurance of any of the above insurance types throughout the term of this Contract. Any increase or decrease in insurance will be as deemed by County of Orange Risk Manager as appropriate to adequately protect County.

County shall notify Contractor in writing of changes in the insurance requirements. If Contractor does not provide acceptable Certificates of Insurance and endorsements to County incorporating such changes within thirty (30) days of receipt of such notice, this Contract may be in breach without further notice to Contractor, 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 Contractor'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.

3. Commercial General Liability

Minimum limits and coverage

$1,000,000 per occurrence; $2,000,000 aggregate

Required Coverage Forms

The Commercial General Liability coverage shall be written on occurrence basis utilizing Insurance Services Office (ISO) form CG 00 01, or a substitute form providing liability 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 20 26 04 13, or a form at least as broad naming the County of Orange its elected and appointed officials, officers, employees, and agents as Additional Insureds, or provide blanket coverage, which will state As Required by Written Contract.

B. A primary non-contributory endorsement using ISO form CG 20 01 04 13, or a form at least as broad evidencing that the Contractor's insurance is primary, and any insurance or self-insurance maintained by the County shall be excess and non-contributing.

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

4. Automobile Liability including coverage for owned, non-owned and hired vehicles

Minimum limits and coverage

$1,000,000 combined Single Limit

Required Coverage Forms

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.

5. Workers Compensation

Minimum limits and coverage

Statutory

Required Endorsements

The Workers' Compensation policy shall contain a waiver of subrogation endorsement waiving all rights of subrogation against the ***County of Orange, its elected and appointed officials, officers, agents, and employees*** or provide blanket coverage, which will state ***As Required by Written Contract.***

6. Employers Liability Insurance

Minimum limits and coverage

$1,000,000 per accident or disease

7. Network Security & Privacy Liability

Minimum limits and coverage

$1,000,000 per claims-made

Required Endorsements

The Network Security and Privacy Liability policy shall contain the following endorsements which shall accompany the Certificate of Insurance:

A. An Additional Insured endorsement naming the ***County of Orange, its elected and appointed officials, officers, agents, and employees*** as Additional Insureds for its vicarious liability.

B. A primary and non-contributory endorsement evidencing that the Contractor's insurance is primary, and any insurance or self-insurance maintained by the County of Orange shall be excess and non-contributing.

If Contractor's Network Security & Privacy Liability is a "Claims-Made" policy, Contractor shall agree to the following:

A. The retroactive date must be shown and must be before the date of the contract or the beginning of the Contract services.

B. Insurance must be maintained, and evidence of insurance must be provided for at least three (3) years after expiration or earlier termination of Contract services.

C. If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a retroactive date prior to the effective date of the contract services, Contractor must purchase an extended reporting period for a minimum of three (3) years after expiration of earlier termination of the Contract.

8. Technology Errors & Omissions

Minimum limits and coverage

$1,000,000 per claims-made; $1,000,000 aggregate

Required Endorsements

If Contractor's Technology Errors & Omissions is a "Claims-Made" policy, Contractor shall agree to the following:

A. The retroactive date must be shown and must be before the date of the contract or the beginning of the Contract services.

B. Insurance must be maintained, and evidence of insurance must be provided for at least three (3) years after expiration or earlier termination of Contract services.

C. If coverage is canceled or non-renewed, and not replaced with another claims-made policy form

with a retroactive date prior to the effective date of the contract services, Contractor must purchase an extended reporting period for a minimum of three (3) years after expiration of earlier termination of the Contract.

ADDITIONAL TERMS AND CONDITIONS

1. Scope of Contract:

This Contract specifies contractual terms and conditions by which County will procure On-Line Marketplace for Cloud Services and Software Items from Contractor as further detailed in the Scope of Work, identified and incorporated herein by this reference as "Attachment A".

2. Term of Contract:

This Contract shall commence upon execution of all necessary signatures and continue for five (5) calendar years from that date, unless otherwise terminated by County. This Contract may be renewed as set forth in the Article titled "Renewal" below.

3. Renewal:

This contract shall not be renewed unless otherwise approved by the County Board of Supervisors.

4. Adjustments – Scope of Work:

No adjustments made to the Scope of Work will be authorized without prior written approval of County assigned Deputy Purchasing Agent.

5. Bills and Liens:

Contractor shall pay promptly all indebtedness for labor, materials and equipment used in performance of the work. Contractor shall not permit any lien or charge to attach to the work or the premises, but if any does so attach, Contractor shall promptly procure its release and, in accordance with the requirements of Article "Indemnification" above, indemnify, defend, and hold County harmless and be responsible for payment of all costs, damages, penalties and expenses related to or arising from or related thereto.

6. Breach of Contract:

The failure of Contractor to comply with any of the provisions, covenants or conditions of this Contract shall be a material breach of this Contract. In such event County may, and in addition to any other remedies available at law, in equity, or otherwise specified in this Contract:

a. Terminate Contract immediately, pursuant to the General Terms and Conditions section, "Termination" Article herein;

b. Afford Contractor written notice of the breach and ten (10) calendar days or such shorter time that may be specified in this Contract within which to cure the breach;

c. Discontinue payment to the Contactor for and during the period in which Contractor is in breach; and

d. Offset against any monies billed by Contractor but yet unpaid by County those monies

disallowed pursuant to the above.

7. Civil Rights:

Contractor attests that services provided shall be in accordance with the provisions of Title VI and Title VII of the Civil Rights Act of 1964, as amended, Section 504 of the Rehabilitation Act of 1973, as amended; the Age Discrimination Act of 1975 as amended; Title II of the Americans with Disabilities Act of 1990, and other applicable State and federal laws and regulations prohibiting discrimination on the basis of race, color, national origin, ethnic group identification, age, religion, marital status, sex or disability.

8. Conflict of Interest – Contractor's Personnel:

Contractor shall exercise reasonable care and diligence to prevent any actions or conditions that could result in a conflict with the best interests of County. This obligation shall apply to Contractor, Contractor's officers, directors, employees, agents, and subcontractors associated with accomplishing work and services hereunder. Contractor's efforts shall include, but not be limited to establishing precautions to prevent its employees, agents, and subcontractors from providing or offering gifts, entertainment, payments, loans or other considerations which could be deemed to influence or appear to influence County staff or elected officers from acting in the best interests of County.

Contractor shall notify County, in writing, of any potential or actual conflicts of interest between Contractor and County that may arise prior to, or during the period of, Contract performance, including, but not limited to, whether any known County public officer's child is an officer or director of, or has an ownership interest of ten (10) percent or more in, Contractor. While Contractor will be required to provide this information without prompting from County any time there is a change regarding conflict of interest, Contractor must also provide an update to County upon request by County.

9. Conflict of Interest – County Personnel:

County of Orange Board of Supervisors policy prohibits its employees from engaging in activities involving a conflict of interest. Contractor shall not, during the period of this Contract, employ any County employee for any purpose.

10. Contractor's Project Manager and Key Personnel:

Contractor shall appoint a Project Manager to direct Contractor's efforts in fulfilling Contractor's obligations under this Contract. This Project Manager shall be subject to approval by County and shall not be changed without the written consent of County's Project Manager, which consent shall not be unreasonably withheld.

Contractor's Project Manager shall be assigned to this project for the duration of Contract and shall diligently pursue all work and services to meet the project time lines. County's Project Manager shall have the right to require the removal and replacement of Contractor's Project Manager from providing services to County under this Contract. County's Project manager shall notify Contractor in writing of such action. Contractor shall accomplish the removal within five (5) business days after written notice by County's Project Manager. County's Project Manager shall review and approve the appointment of the replacement for Contractor's Project Manager. County is not required to provide any additional information, reason or rationale in the event it requires the removal of Contractor's Project Manager from providing further services under Contract.

11. Contractor Personnel – Reference Checks:

Contractor warrants that all persons employed to provide service under this Contract have satisfactory past work records indicating their ability to adequately perform the work under this Contract. Contractor's employees assigned to this project must meet character standards as demonstrated by background investigation and reference checks, coordinated by the agency/department issuing this Contract.

12. Contractor's Expense:

The Contractor will be responsible for all costs related to photo copying, telephone communications, fax communications, and parking while on County sites during the performance of work and services under this Contract. The County will not provide free parking for any service in the County Civic Center.

13. Contractor's Records:

Contractor shall keep true and accurate accounts, records, books and data which shall correctly reflect the business transacted by Contractor in accordance with generally accepted accounting principles. These records shall be stored in Orange County for a period of three (3) years after final payment is received from County. Storage of records in another county will require written approval from County of Orange assigned Deputy Purchasing Agent.

14. Conditions Affecting Work:

Contractor shall be responsible for taking all steps reasonably necessary to ascertain the nature and location of the work to be performed under this Contract and to know the general conditions which can affect the work or the cost thereof. Any failure by Contractor to do so will not relieve Contractor from responsibility for successfully performing the work without additional cost to County. 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 execution of this Contract, unless such understanding or representations by County are expressly stated in Contract.

15. Cooperative Contract:

This Contract is a cooperative contract and may be utilized by all County of Orange departments.

The provisions and pricing of this Contract may be extended, at the option of Contractor, to any Municipal, County, Public Utility, Hospital, Educational Institution, or any other non-profit or governmental organization (the "Cooperative Program"). Parties in a Cooperative Program wishing to use this Contract will be responsible for issuing their own purchase documents / price agreements, providing for their own acceptance, and making any subsequent payments. Contractor shall be required to include in any agreement entered into with another agency or entity that is entered into pursuant to the provisions and pricing of this Contract a clause that binds the parties to the agreement to "indemnify, defend with counsel approved in writing by the County of Orange, California ("County"), and hold County, its elected and appointed officials, officers, employees, agents and those special districts and agencies which County's Board of Supervisors acts as the governing Board ("County Indemnitees") harmless from any claims, demands or liability of any kind or nature, including but not limited to personal injury or property damage, arising from or related to the services, products or other performance provided" under the agreement.. Failure to so include this clause voids the Contract's extension to a Cooperative Program and will be considered a material breach of this Contract and grounds for immediate Contract termination. The cooperative entities

are responsible for obtaining all certificates of insurance and bonds required. The County of Orange makes no guarantee of usage by other users of this Contract.

As a cost-recovery mechanism for County, a 2 percent administrative rebate on total sales from all subordinate contracts will be paid to the County for any contracts the Contractor agrees to enter into with another agency or entity, other than the County of Orange or a department thereof, under the provisions and pricing of this Contract. The County has partnered with Pavilion, a third-party administrator, responsible for managing all reporting and payments under this Cooperative Program. The Contractor shall provide quarterly Volume Sales Reports about additional sales to other entities under the provisions and pricing of this Contract. The Reports shall include the ordering agency, detail of items sold including description, quantity, and price, and shall include all transactions pertaining to sales under the Contract provisions and pricing for that Reporting Period. Contractor shall provide the Volume Sales Reports regardless of whether or not any sales have been conducted. Failure of the Contractor to provide quarterly reports as required may be deemed by the County as a material breach of the Contract. A late penalty of 15 percent on the value of the rebate may be assessed to the Contractor for each month the payments are not received.

Subordinate contracts must be executed prior to the expiration or earlier termination of this Contract and may survive the expiration of this Contract. This Cooperative Contract provision shall survive expiration or termination of this Contract.

16. Data – Title To:

All materials, documents, data or information obtained from County data files or any County medium furnished to Contractor in the performance of this Contract will at all times remain the property of County. Such data or information may not be used or copied for direct or indirect use by Contractor after completion or termination of this Contract without the express written consent of County. All materials, documents, data or information, including copies, must be returned to County at the end of this Contract.

17. Default – Re-Procurement Costs:

In case of Contract breach by Contractor, resulting in termination by County, County may procure the commodities and services from other sources. If the cost for those commodities and services is higher than under the terms of the existing Contract, Contractor will be responsible for paying County the difference between Contract cost and the price paid, and County may deduct this cost from any unpaid balance due Contractor. The price paid by County shall be the prevailing market price at the time such purchase is made. This is in addition to any other remedies available under this Contract and under law.

18. Disputes – Contract:

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 the Contractor's Project Manager and the County's Project Manager, as specified in Article titled "Notices" below, such matter shall be brought to the attention of the County DPA by way of the following process:

A. The Contractor shall submit to the agency/department assigned Deputy Purchasing Agent 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 County, on its own initiative, has already rendered such a final decision.

B. The Contractor's written demand shall be fully supported by factual information, and, if such demand involves a cost adjustment to Contract, Contractor 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 Contract adjustment for which Contractor believes County is liable.

Pending the final resolution of any dispute arising under, related to, or involving this Contract, Contractor agrees to diligently proceed with the performance of this Contract, including the delivery of commodities and/or provision of services. Contractor's failure to diligently proceed shall be considered a material breach of this Contract.

Any final decision of County shall be expressly identified as such, shall be in writing, and shall be signed by County Deputy Purchasing Agent or his designee. If County fails to render a decision within 90 days after receipt of Contractor's demand, it shall be deemed a final decision adverse to Contractor's contentions. Nothing in this section shall be construed as affecting County's right to terminate Contract for cause or termination for convenience as stated in Article "Termination" herein.

19. Drug-Free Workplace:

Contractor hereby certifies compliance with Government Code Section 8355 in matters relating to providing a drug-free workplace. Contractor will:

A. Publish a statement notifying employees that unlawful manufacture, distribution, dispensation, possession, or use of a controlled substance is prohibited and specifying actions to be taken against employees for violations, as required by Government Code Section 8355(a)(1).

B. Establish a drug-free awareness program as required by Government Code Section 8355(a)(2) to inform employees about all of the following:

1. The dangers of drug abuse in the workplace;
2. The organization's policy of maintaining a drug-free workplace
3. Any available counseling, rehabilitation and employee assistance programs; and
4. Penalties that may be imposed upon employees for drug abuse violations.

C. Provide as required by Government Code Section 8355(a)(3) that every employee who works under this Contract:

1. Will receive a copy of the company's drug-free policy statement; and
2. Will agree to abide by the terms of the company's statement as a condition of employment under this Contract.

D. Failure to comply with these requirements may result in suspension of payments under Contract or termination of Contract or both, and Contractor may be ineligible for award of any future County contracts if County determines that any of the following has occurred:

1. Contractor has made false certification, or
2. Contractor violates the certification by failing to carry out the requirements as noted above.

20. EDD Independent Contractor Reporting Requirements:

Effective January 1, 2001, County of Orange is required to file in accordance with subdivision (a) of Section 6041A of the Internal Revenue Code for services received from a "service provider" to whom County pays $600 or more or with whom County enters into a contract for $600 or more within a single calendar year. The purpose of this reporting requirement is to increase child support collection by helping to locate parents who are delinquent in their child support obligations.

The term "service provider" is defined in California Unemployment Insurance Code Section 1088.8, subparagraph B.2 as "an individual who is not an employee of the service recipient for California purposes and who received compensation or executes a contract for services performed for that service recipient within or without the state." The term is further defined by the California Employment Development Department to refer specifically to independent Contractors. An independent Contractor is defined as "an individual who is not an employee of the ... government entity for California purposes and who receives compensation or executes a contract for services performed for that ... government entity either in or outside of California."

The reporting requirement does not apply to corporations, general partnerships, limited liability partnerships, and limited liability companies.

Additional information on this reporting requirement can be found at the California Employment Development Department website located at http://www.edd.ca.gov/Employer_Services.htm

21. Emergency/Declared Disaster Requirements:

In the event of an emergency or if Orange County is declared a disaster area by County, state or federal government, Contract may be subjected to unusual usage. Contractor shall service County during such an emergency or declared disaster under the same terms and conditions that apply during non-emergency/disaster conditions. The pricing quoted by Contractor shall apply to serving County's needs regardless of the circumstances. If Contractor is unable to supply the goods/services under the terms of Contract, then Contractor shall provide proof of such disruption and a copy of the invoice for the goods/services from Contractor's supplier(s). Additional profit margin as a result of supplying goods/services during an emergency or a declared disaster shall not be permitted. In the event of an emergency or declared disaster, emergency purchase order numbers will be assigned. All applicable invoices from Contractor shall show both the emergency purchase order number and Contract number.

22. Error and Omissions:

All reports, files and other documents prepared and submitted by Contractor shall be complete and shall be carefully checked by the professional(s) identified by Contractor as Project Manager and key personnel attached hereto, prior to submission to the County. Contractor agrees that County review is discretionary, and Contractor shall not assume that the County will discover errors and/or omissions. If the County discovers any errors or omissions prior to approving Contractor's reports, files and other written documents, the reports, files or documents will be returned to Contractor for correction. Should the County or others discover errors or omissions in the reports, files or other written documents submitted by the Contractor after County approval thereof, County approval of Contractor's reports, files or documents shall not be used as a defense by Contractor in any action between the County and Contractor, and the reports, files or documents will be returned to Contractor for correction.

23. Equal Employment Opportunity:

Contractor shall comply with U.S. Executive Order 11246 entitled, "Equal Employment Opportunity" as amended by Executive Order 11375 and as supplemented in Department of Labor regulations (41 CFR, Part 60) and applicable state of California regulations as may now exist or be amended in the future. Contractor shall not discriminate against any employee or applicant for employment on the basis of race, color, national origin, ancestry, religion, sex, marital status, political affiliation or physical or mental condition.

Regarding handicapped persons, Contractor will not discriminate against any employee or applicant for employment because of physical or mental handicap in regard to any position for which the employee or applicant for employment is qualified. Contractor agrees to provide equal opportunity to handicapped persons in employment or in advancement in employment or otherwise treat qualified handicapped individuals without discrimination based upon their physical or mental handicaps in all employment practices such as the following: employment, upgrading, promotions, transfers, recruitments, advertising, layoffs, terminations, rate of pay or other forms of compensation, and selection for training, including apprenticeship. Contractor agrees to comply with the provisions of Sections 503 and 504 of the Rehabilitation Act of 1973, as amended, pertaining to prohibition of discrimination against qualified handicapped persons in all programs and/or activities as detailed in regulations signed by the Secretary of the Department of Health and Human Services effective June 3, 1977, and found in the Federal Register, Volume 42, No. 68 dated May 4, 1977, as may now exist or be amended in the future.

Regarding Americans with disabilities, Contractor agrees to comply with applicable provisions of Title 1 of the Americans with Disabilities Act enacted in 1990 as may now exist or be amended in the future.

24. Headings:

The various headings and numbers herein, the grouping of provisions of this Contract into separate clauses and articles, and the organization hereof are for the purpose of convenience only and shall not limit or otherwise affect the meaning hereof.

25. News/Information Release:

Contractor agrees that it will not issue any news releases in connection with either the award of this Contract or any subsequent amendment of or effort under this Contract without first obtaining review and written approval of said news releases from County through County's Project Manager.

26. Notices:

Any and all notices, requests demands and other communications contemplated, called for, permitted, or required to be given hereunder shall be in writing with a copy provided to the assigned DPA, except through the course of the Parties' Project Managers' routine exchange of information and cooperation during the terms of the work and services. Any written communications shall be deemed to have been duly given upon actual in-person delivery, if delivery is by direct hand, or upon delivery on the actual day of receipt or no greater than four (4) calendar days after being mailed by US certified or registered mail, return receipt requested, postage prepaid, whichever occurs first. The date of mailing shall count as the first day. All communications shall be addressed to the appropriate party at the address stated herein or such other address as the Parties hereto may designate by written notice from time to time in the manner aforesaid.

Contractor:	Carahsoft Technology Corp
Attn:	Ian Edington
Address:	11493 Sunset Hills Road, Suite 100 Reston, VA 20190
Phone:	(571) 662-4584
Email:	Ian.Edington@carahsoft.com

cc: County Procurement Office/Procurement Services	
Attn:	Christina Rojas, County DPA
Address:	400 West Civic Center Dr. 5th Floor Santa Ana, CA 92701
Phone:	(714) 567-7368
Email:	christina.rojas@ocgov.com

27. Precedence:

Contract documents consist of this Contract and its exhibits and attachments. In the event of a conflict between or among Contract documents, the order of precedence shall be the provisions of the main body of this Contract, i.e., those provisions set forth in the recitals and articles of this Contract, and then the exhibits and attachments.

28. Subcontracting:

No performance of this Contract or any portion thereof may be subcontracted or otherwise delegated by Contractor, in whole or in part, without first obtaining the prior express written consent of County. Any attempt by Contractor to subcontract or delegate any performance of this Contract without the prior express written consent of County shall be invalid and shall constitute a material breach of this Contract, and any attempted assignment or delegation in derogation of this paragraph shall be void.

In the event that Contractor is authorized by County to subcontract, this Contract shall take precedence over the terms of the agreement between Contractor and subcontractor, and any agreement between Contractor and a subcontractor shall incorporate by reference the terms of this Contract. Contractor shall remain responsible for the performance of this Contract and indemnification of County notwithstanding the County's consent to Contractor's request for approval of a subcontractor. Under no circumstances shall County be required to directly monitor the performance of any subcontractor. All work performed by a subcontractor must be monitored by Contractor and must meet the approval of the County of Orange pursuant to the terms of this Contract.

29. Termination – Orderly:

After receipt of a termination notice from County of Orange, Contractor may submit to County a termination claim, if applicable. Such claim shall be submitted promptly, but in no event later than 60 days from the effective date of the termination, unless one or more extensions in writing are granted by County upon written request of Contractor. Upon termination County agrees to pay Contractor for all services performed prior to termination which meet the requirements of Contract, provided, however, that such compensation combined with previously paid compensation shall not exceed the total compensation set forth in Contract. Upon 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 Contract.

30. Usage:

No guarantee is given by County to Contractor regarding usage of this Contract. Usage figures, if provided, are approximations. Contractor agrees to supply services and/or commodities requested, as needed by County of Orange, at rates/prices listed in Contract, regardless of quantity requested.

31. Usage Reports:

Contractor shall submit usage reports on an annual basis to the assigned Deputy Purchasing Agent of County of Orange user agency/department. The usage report shall be in a format specified by the user agency/department and shall be submitted 90 days prior to the expiration date of Contract term, or any subsequent renewal term, if applicable.

32. County of Orange Local Small Business Preference Requirements:

Contractor certifies it is in compliance with the applicable County of Orange Local Small Business (OCLSB) and Disabled Veteran Business Enterprise (DVBE) Preference requirements at the time of bid/proposal submittal.

If applicable, Contractor certifies that OCLSB and/or DVBE Subcontractor(s) specified in Attachment "Staffing Plan" comply with County's OCLSB and/or DVBE Preference at the time of bid/proposal submittal and shall ensure that at least 20% of the Contract amount is allocated to OCLSB and/or DVBE Subcontractor(s) as specified in Attachment.

For Public Works contracts, if applicable, Contractor will ensure that at least 3% of the Contract amount is allocated to OCLSB and/or DVBE Subcontractor(s), as specified in Attachment "Staffing Plan".

33. Disabled Veteran Business Enterprise Preference Requirements:

Contractor certifies it is in compliance with County of Orange Disabled Veteran Business Enterprise Preference requirements at the time this Contract is executed.

34. Project Manager, County:

The County shall appoint a Project Manager to act as liaison between the County and the Contractor during the term of this Contract. The County's Project Manager shall coordinate the activities of the County staff assigned to work with the Contractor.

The County's Project Manager shall have the right to require the removal and replacement of the Contractor's Project Manager and key personnel. The County's Project Manager shall notify the Contractor

in writing of such action. The Contractor shall accomplish the removal within three (3) business days after written notice from the County's Project Manager. The County's Project Manager shall review and approve the appointment of the replacement for the Contractor's Project Manager and key personnel. Said approval shall not be unreasonably withheld. The County is not required to provide any additional information, reason or rationale in the event it requires the removal of Contractor's Project Manager from providing further services under the Contract.

35. Mandatory Kick-Off Meeting:

Upon award of the contract, the awarded vendor(s) may be required to attend a mandatory kick-off meeting with County representatives to discuss important information related to the scope of work, the contract, and the invoice payment process. A quarterly check-in meeting may be required to review any issues with the contract.

36. Permits and Licenses:

Contractor shall be required to obtain any and all approvals, permits and/or licenses which may be required in connection with the permitted operation as set out herein. No permit approval or consent given hereunder by County in its governmental capacity shall affect or limit Contractor's obligations hereunder, nor shall any approvals or consents given by County as a party to this Contract, be deemed approval as to compliance or conformance with applicable governmental codes, laws, ordinances, rules, or regulations.

37. Inventory:

County has an ongoing requirement for the commodities indicated in this Contract. Contractor shall maintain a reasonable stock on hand of all commodities for delivery upon request.

38. Order Dates:

Orders may be placed during the term of Contract even if delivery may not be made until after the term of Contract. Order dates take precedence over delivery dates. Contract must clearly identify the order date on all invoices to County.

INFORMATION TECHNOLOGY ADDITIONAL TERMS AND CONDITIONS

1. Software License

Unless otherwise specified in the Scope of Work, the Contractor hereby grants to the County and the County accepts from the Contractor, subject to the terms and conditions of this Contract, an irrevocable, royalty-free, non-exclusive, license to use all Software of any type provided by Contractor to County.

2. Future Releases

Unless otherwise specifically provided in this Contract, or the Scope of Work, if improved versions, e.g., patches, bug fixes, Updates or releases, of any solution are developed by the Contractor, and are made available to other licensees, they will be made available to the County at no additional cost only if such are made available to other licensees at no additional cost. If the Contractor offers new versions or Upgrades to the solution, they shall be made available to the County at the County's option at a price no greater than the Contract price plus a price increase proportionate to the increase from the list price of the original version to that of the new version, if any. If the Software product has no list price, such price increase will be proportionate to the increase in average price from the original to the new version, if any, as estimated by the Contractor in good faith.

3. Software Maintenance

The correction of any residual errors in any software products which may be discovered by the Contractor or by the County will be considered maintenance. Such maintenance will be performed by the contractor without additional charge for the duration of this Contract. The contractor will be available to assist the County in isolating and correcting error conditions caused by the County's particular hardware or operating system at rates specified in this contract. If the contractor is called upon by the state to correct an error caused by the County's negligence, modification by the County, County-supplied data, or machine or operator failure or due to any other cause not inherent in the original software products, the contractor reserves the right to charge the County for such service on a time and material basis at rates in accordance with the contract.

4. County Data

Subject to applicable law, the County shall permit the Contractor and its subcontractors to have access to, and make appropriate use of, the information or material that the County submits to the Contractor pursuant to this Contract ("County Data"), solely to the extent the Contractor requires such access and use in order to properly and appropriately perform the Services as contemplated by this Contract. The Contractor 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. The Contractor 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.

5. Acceptance Testing

All Deliverables shall be provided to the County by the Contractor in conformity with all requirements, specifications, Acceptance Criteria, and time periods set forth or referenced in this Contract. The Contractor 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 in mutual agreement by the County's Project Manager and Contractor's Project Owner, and no such activities shall be deemed completed until all Acceptance Criteria, whether set forth in this Contract or mutually agreed upon by the

Parties in writing, have been successfully met. Moreover, nothing in this section shall limit in any way the County's right to terminate immediately for cause pursuant to Paragraph 11, Termination, herein.

A. Acceptance Testing: Following the Contractor's notification to the County that the Contractor has completed any component or Deliverable identified in this Contract, at a mutually agreed scheduled time thereafter, the 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 the County has completed such testing or upon expiration of the agreed-upon testing period or any agreed-upon extension of the testing period (the "Acceptance Testing Period"), the County shall notify the Contractor in writing either that the component or Deliverable: (a) meets the Acceptance Criteria and that acceptance of such component or Deliverable has occurred ("Acceptance"); or (b) does not meet the Acceptance Criteria 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 the County determines that a component or Deliverable does not conform to the applicable Acceptance Criteria, and that it is in the County's interest to allow the Contractor time to correct the problem, the County shall deliver to the Contractor a written exception report describing the nonconformity (the "Exception Report").
Within ten (10) calendar days following receipt of the Exception Report, the Contractor shall: (a) perform a Root Cause Analysis to identify the cause of the nonconformity; (b) provide the County with a written report detailing the cause of, and procedure for correcting, such nonconformity; (c) provide the County with satisfactory evidence that such nonconformity will not recur; and (d) use best efforts to correct critical errors (as determined by the County) and use commercially reasonable efforts to correct all other errors reasonably requested by the County and accepted by the Contractor; 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, the Contractor shall present to the County a mutually agreeable plan to cure such nonconformity within a reasonable amount of time. Upon the Contractor's notice to the County that the Contractor has cured any such nonconformity, the 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 subsections (a) through (c) above shall be repeated. In the event the County rejects the component or Deliverable a second time and the Contractor 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, the 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 the County has completed such testing or upon expiration of the testing period (the "Final Acceptance Testing Period"), the County shall notify the Contractor in writing that the System, and all components and Deliverables that are a part thereof: (a) meet the Acceptance Criteria and that final acceptance of the System and such components and Deliverables has occurred ("Final Acceptance"); or (b) does not meet the Acceptance Criteria and the reasons therefor. If the 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 the County shall constitute a waiver by the 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 the County's Final Acceptance thereof. Nothing else, including the County's use of the System, or any component thereof, shall constitute Final Acceptance, affect any rights and remedies that may be available to the County and/or constitute or result in "acceptance" under general contract law, any state uniform commercial code or any other law.

6. Compatibility of Resources

The Contractor shall ensure that the solution Software, all Services, and all Software, assets, Hardware, Equipment, and other resources and materials (collectively, the "Contractor Resources") that are provided by the Contractor to the County, otherwise utilized by the Contractor, or approved by the Contractor for utilization by the County, in connection with the use or operation of the solution, 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 Contractor Resources to integrate fully and successfully and be compatible with the County Resources, the Contractor 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.

7. Monitoring and Measuring Tools and Processes

The Contractor shall implement measurement and monitoring tools and produce the metrics and reports necessary to measure its performance against any of the SLRs and shall deliver to the County such reports in accordance with the frequency set forth in Attachment G – Performance, Service Level Guarantees, and Reporting the Contract. Upon request in connection with an audit, and at no additional charge to the County, the Contractor shall provide the County or its designees with information and access to tools and procedures used to produce such metrics.

8. Data Location

Except where the Contractor obtains the County's prior written approval, the physical location of the Contractor's data center where County Data is stored shall be within the United States.

9. Disentanglement Process

In the event of expiration of the Term or termination of this Contract, in whole or in part, the Contractor will perform disentanglement services to transition responsibility for the provision of Services to a replacement contractor or to the County itself ("Disentanglement Services"). The Disentanglement Services shall begin on the expiration date of the Term or termination date of this Contract and, unless the Parties subsequently agree in writing to extend the Term, the Contractor shall continue to provide Disentanglement Services, in accordance with this Section 43 or as the County reasonably requests, until the earlier of a Disentanglement satisfactory to the County has been completed or twelve (12) months after the expiration of the Term or termination date, as appropriate.

As soon as reasonably practicable after the Disentanglement Services begin, the Contractor and the County shall develop a plan in good faith that specifies the tasks to be performed by the Parties during disentanglement and the schedule for the performance of such tasks. Unless otherwise agreed by the Parties in writing, such plan shall not in any respect lessen or eliminate the Contractor's obligations under this Contract to provide all Disentanglement Services necessary and reasonably requested by the County. The plan will be developed, implemented, and concluded with full disentanglement with all due speed, not to

exceed twelve (12) months.

The Parties shall cooperate fully with one another, and any replacement contractor, to facilitate a smooth transition of the Services from the Contractor to the replacement contractor or the County. The Disentanglement Services will be provided to the County by the Contractor regardless of the reason for termination or expiration. The Contractor shall continue to provide the Services during disentanglement in a manner consistent with the Contractor's provision and performance of such Services during the period such Services were provided to the County hereunder, with no material interruption of the Services and no material adverse impact on the provision of the Services.

All Disentanglement Services performed by the Contractor shall be performed by the Contractor at no additional cost to the County beyond what the County would pay for the Services.

10. Trans-Border Data Flows

Contractor shall not transfer any County Data across a country border.

County of Orange Information Technology Security Provisions

All Contractors with access to County data and/or systems shall establish and maintain policies, procedures, and technical, physical, and administrative safeguards designed to (i) ensure the confidentiality, integrity, and availability of all County data and any other confidential information that the Contractor receives, stores, maintains, processes, transmits, or otherwise accesses in connection with the provision of the contracted services, (ii) protect against any threats or hazards to the security or integrity of County data, systems, or other confidential information, (iii) protect against unauthorized access, use, or disclosure of personal or County confidential information, (iv) maintain reasonable procedures to prevent, detect, respond, and provide notification to the County regarding any internal or external security breaches, (v) ensure the return or appropriate disposal of personal information or other confidential information upon contract conclusion (or per retention standards set forth in the contract), and (vi) ensure that any subcontractor(s)/agent(s) that receives, stores, maintains, processes, transmits, or otherwise accesses County data and/or system(s) is in compliance with statements and the provisions of statements and services herein.

1. This County of Orange Information Technology Security Provisions document provides a high-level guide for contractors to understand the resiliency and cybersecurity expectations of the County. The County of Orange Security Guidelines follow the latest National Institute of Standards and Technology (NIST) 800-53 framework to ensure the highest levels of operational resiliency and cybersecurity.

   Contractor, Contractor personnel, Contractor's subcontractors, any person performing work on behalf of Contractor, and all other agents and representatives of Contractor will, at all times, comply with and abide by all County of Orange Information Technology Security Provisions ("Security Provisions") that pertain to Contractor(s) in connection with the Services performed by Contractor(s) as set forth in the scope of work of this Contract. Any violations of the Security Provisions shall, in addition to all other available rights and remedies available to County, be cause for immediate termination of this Contract. Such Security Provisions include, but are not limited to, Attachment "C" - County of Orange Information Technology Security Guidelines, as applicable, and Attachment "D" - Business Associate Contract.

   Contractor shall use industry best practices and methods with regard to confidentiality, integrity, availability, and the prevention, detection, response, and elimination of threat, by all appropriate means, of fraud, abuse, and other inappropriate or unauthorized access to County data and/or system(s) accessed in the performance of Services under this Contract.

2. The Contractor shall implement and maintain a written information security program that contains reasonable and appropriate security measures designed to safeguard the confidentiality, integrity, availability, and resiliency of County data and/or system(s). The Contractor shall review and update its information security program in accordance with contractual, legal, and regulatory requirements. Contractor shall provide to County a copy of the organization's information security program and/or policies.

3. Information Access: Contractor shall use appropriate safeguards and security measures to ensure the confidentiality and security of all County data.

   County may require all Contractor personnel, subcontractors, and affiliates approved by County to perform work under this Contract to execute a confidentiality and non-disclosure agreement concerning access protection and data security in the form provided by County. County shall

authorize, and Contractor shall issue, any necessary information-access mechanisms, including access IDs and passwords, and in no event shall Contractor permit any such mechanisms to be shared or used by other than the individual Contractor personnel, subcontractor, or affiliate to whom issued. Contractor shall provide each Contractor personnel, subcontractors, or affiliates with only such level of access as is required for such individual to perform his or her assigned tasks and functions.

Throughout the Contract term, upon request from County but at least once each calendar year, Contractor shall provide County with an accurate, up-to-date list of those Contractor personnel and/or subcontractor personnel having access to County systems and/or County data, and the respective security level or clearance assigned to each such Contractor personnel and/or subcontractor personnel. County reserves the right to require the removal and replacement of Contractor personnel and/or subcontractor personnel at the County's sole discretion. Removal and replacement shall be performed within 14 calendar days of notification by the County.

All County resources (including County systems), County data, County hardware, and County software used or accessed by Contractor: (a) shall be used and accessed by such Contractor and/or subcontractors personnel solely and exclusively in the performance of their assigned duties in connection with, and in furtherance of, the performance of Contractor's obligations hereunder; and (b) shall not be used or accessed except as expressly permitted hereunder, or commercially exploited in any manner whatsoever, by Contractor or Contractor's personnel and subcontractors, at any time.

Contractor acknowledges and agrees that any failure to comply with the provisions of this paragraph shall constitute a breach of this Contract and entitle County to deny or restrict the rights of such non-complying Contractor personnel and/or subcontractor personnel to access and use the County data and/or system(s), as County in its sole discretion shall deem appropriate.

4. Data Security Requirements: Without limiting Contractor's obligation of confidentiality as further described in this Contract, Contractor must establish, maintain, and enforce a data privacy program and an information and cyber security program, including safety, physical, and technical security and resiliency policies and procedures, that comply with the requirements set forth in this Contract and, to the extent such programs are consistent with and not less protective than the requirements set forth in this Contract and are at least equal to applicable best industry practices and standards (NIST 800-53).

   Contractor also shall provide technical and organizational safeguards against accidental, unlawful, or unauthorized access or use, destruction, loss, alteration, disclosure, transfer, commingling, or processing of such information that ensure a level of security appropriate to the risks presented by the processing of County Data,

   Contractor personnel and/or subcontractor personnel and affiliates approved by County to perform work under this Contract may use or disclose County personal and confidential

   information only as permitted in this Contract. Any other use or disclosure requires express approval in writing by the County of Orange. No Contractor personnel and/or subcontractor personnel or affiliate shall duplicate, disseminate, market, sell, or disclose County personal and confidential information except as allowed in this Contract. Contractor personnel and/or subcontractor personnel or affiliate who access, disclose, market, sell, or use County personal and confidential information in a manner or for a purpose not authorized by this Contract may be subject

to civil and criminal sanctions contained in applicable federal and state statutes.

Contractor shall take all reasonable measures to secure and defend all locations, equipment, systems, and other materials and facilities employed in connection with the Services against hackers and others who may seek, without authorization, to disrupt, damage, modify, access, or otherwise use Contractor systems or the information found therein; and prevent County data from being commingled with or contaminated by the data of other customers or their users of the Services and unauthorized access to any of County data.

Contractor shall also continuously monitor its systems for potential areas where security could be breached. In no case shall the safeguards of Contractor's data privacy and information and cyber security program be less stringent than the safeguards used by County. Without limiting any other audit rights of County, County shall have the right to review Contractor's data privacy and information and cyber security program prior to commencement of Services and from time to time during the term of this Contract.

All data belongs to the County and shall be destroyed or returned at the end of the contract via digital wiping, degaussing, or physical shredding as directed by County.

5. Enhanced Security Measures: County may, in its discretion, designate certain areas, facilities, or solution systems as ones that require a higher level of security and access control. County shall notify Contractor 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 Contractor shall be required to implement and enforce, as well as the date on which such procedures and measures shall take effect. Contractor shall and shall cause Contractor personnel and subcontractors to fully comply with and abide by all such enhanced security and access measures and procedures as of such date.

6. General Security Standards: Contractor will be solely responsible for the information technology infrastructure, including all computers, software, databases, electronic systems (including database management systems, email systems, auditing, and monitoring systems) and networks used by or for Contractor ("Contractor Systems") to access County resources (including County systems), County data or otherwise in connection with the Services and shall prevent unauthorized access to County resources (including County systems) or County data through the Contractor Systems.

   a) **Contractor System(s) and Security:** At all times during the contract term, Contractor shall maintain a level of security with regard to the Contractor Systems, that in all events is at least as secure as the levels of security that are common and prevalent in the industry and in accordance with industry best practices (NIST 800-53). Contractor shall maintain all appropriate administrative, physical, technical, and procedural safeguards to secure County data from data breach, protect County data and the Services from loss, corruption, unauthorized disclosure, and from hacks, and the introduction of viruses, disabling devices, malware, and other forms of malicious and inadvertent acts that can disrupt County's access and use of County data and the Services.

   b) **Contractor and the use of Email:** Contractor, including Contractor's employees and subcontractors, that are provided a County email address must only use the County email system for correspondence of County business. Contractor, including Contractor's employees and subcontractors, must not access or use personal, non-County Internet (external) email

systems from County networks and/or County computing devices. If at any time Contractor's performance under this Contract requires such access or use, Contractor must submit a written request to County with justification for access or use of personal, non-County Internet (external) email systems from County networks and/or computing devices and obtain County's express prior written approval.

Contractors who are not provided with a County email address, but need to transmit County data will be required to maintain and transmit County data in accordance with this Agreement.

7. Security Failures: Any failure by the Contractor to meet the requirements of this Contract with respect to the security of County data, including any related backup, disaster recovery, or other policies, practices or procedures, and any breach or violation by Contractor or its subcontractors or affiliates, or their employees or agents, of any of the foregoing, shall be deemed a material breach of this Contract and may result in termination and reimbursement to County of any fees prepaid by County prorated to the date of such termination. The remedy provided in this paragraph shall not be exclusive and is in addition to any other rights and remedies provided by law or under the Contract.

8. Security Breach Notification: In the event Contractor becomes aware of any act, error or omission, negligence, misconduct, or security incident including unsecure or improper data disposal, theft, loss, unauthorized use and disclosure or access, that compromises or is suspected to compromise the security, availability, confidentiality, and/or integrity of County data or the physical, technical, administrative, or organizational safeguards required under this Contract that relate to the security, availability, confidentiality, and/or integrity of County data, Contractor shall, at its own expense, (1) immediately (or within 24 hours of potential or suspected breach), notify the County's Chief Information Security Officer and County Privacy Officer of such occurrence; (2) perform a root cause analysis of the actual, potential, or suspected breach; (3) provide a remediation plan that is acceptable to County within 30 days of verified breach, to address the occurrence of the breach and prevent any further incidents; (4) conduct a forensic investigation to determine what systems, data, and information have been affected by such event; and (5) cooperate with County and any law enforcement or regulatory officials investigating such occurrence, including but not limited to making available all relevant records, forensics, investigative evidence, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by County and/or any law enforcement or regulatory officials, and (6) perform or take any other actions required to comply with applicable law as a result of the occurrence (at the direction of County).

   County shall make the final decision on notifying County officials, entities, employees, service providers, and/or the general public of such occurrence, and the implementation of the remediation plan. If notification to particular persons is required under any law or pursuant to any of County's privacy or security policies, then notifications to all persons and entities who are affected by the same event shall be considered legally required. Contractor shall reimburse County for all notification and related costs incurred by County arising out of or in connection with any such occurrence due to Contractor's acts, errors or omissions, negligence, and/or misconduct resulting in a requirement for legally required notifications.

   In the case of a breach, Contractor shall provide third-party credit and identity monitoring services to each of the affected individuals for the period required to comply with applicable law, or, in the

absence of any legally required monitoring services, for no less than twelve (12) months following the date of notification to such individuals.

Contractor shall indemnify, defend with counsel approved in writing by County, and hold County and County Indemnitees harmless from and against any and all claims, including reasonable attorney's fees, costs, and expenses incidental thereto, which may be suffered by, accrued against, charged to, or recoverable from County in connection with the occurrence.

Notification shall be sent to:

Andrew Alipanah, MBA, CISSP
Chief Information Security Officer
721 S. Parker St.
Suite 200
Orange, CA 92868
Phone: (714) 567-7611
Andrew.Alipanah@ocit.ocgov.com

Linda Le, CHPC, CHC, CHP
County Privacy Officer
721 S. Parker St.
Suite 200
Orange, CA 92868
Phone: (714) 834-4082
Linda.Le@ocit.ocgov.com

9. Security Audits: Contractor shall maintain complete and accurate records relating to its system and Organization Controls (SOC) Type II audits or equivalent's data protection practices, internal and external audits, and the security of any of County-hosted content, including any confidentiality, integrity, and availability operations (data hosting, backup, disaster recovery, external dependencies management, vulnerability testing, penetration testing, patching, or other related policies, practices, standards, or procedures).

   Contractor shall inform County of any internal/external security audit or assessment performed on Contractor's operations, information and cyber security program, disaster recovery plan, and prevention, detection, or response protocols that are related to hosted County content, within sixty (60) calendar days of such audit or assessment. Contractor will provide a copy of the audit report to County within thirty (30) days after Contractor's receipt of request for such report(s).

   Contractor shall reasonably cooperate with all County security reviews and testing, including but not limited to penetration testing of any cloud-based solution provided by Contractor to County under this Contract. Contractor shall implement any required safeguards as identified by County or by any audit of Contractor's data privacy and information/cyber security program.

   In addition, County has the right to review Plans of Actions and Milestones (POA&M) for any outstanding items identified by the SOC 2 Type II report requiring remediation as it pertains to the confidentiality, integrity, and availability of County data. County reserves the right, at its sole discretion, to immediately terminate this Contract or a part thereof without limitation and without liability to County if County reasonably determines Contractor fails or has failed to meet its obligations under this section.

10. Business Continuity and Disaster Recovery (BCDR):

    For the purposes of this section, "Recovery Point Objectives" means the maximum age of files (data and system configurations) that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a hardware, program, or communications failure (establishing the data backup schedule and strategy). "Recovery Time Objectives" means the maximum duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences

associated with a loss of functionality.

The Contractor shall maintain a comprehensive risk management program focused on managing risks to County operations and data, including mitigation of the likelihood and impact of an adverse event occurring that would negatively affect contracted services and operations of the County. Business continuity management will enable the Contractor to identify and minimize disruptive risks and restore and recover hosted County business-critical services and/or data within the agreed terms following an adverse event or other major business disruptions. Recovery and timeframes may be impacted when events or disruptions are related to dependencies on third- parties. The County and Contractor will agree on Recovery Point Objectives and Recovery Time Objectives (as needed)) and will periodically review these objectives. Any disruption to services of system will be communicated to the County within 4 hours, and every effort shall be undertaken to restore contracted services, data, operations, security, and functionality.

All data and/or systems and technology provided by the Contractor internally and through third-party vendors shall have resiliency and redundancy capabilities to achieve high availability and data recoverability. Contractor Systems shall be designed, where practical and possible, to ensure continuity of service(s) in the event of a disruption or outage.

SIGNATURE PAGE

IN WITNESS WHEREOF, the Parties hereto have executed this Contract on the date following their respective signatures.

Carahsoft Technology Corp, a Corporation in Maryland

Signature	Name	Title	Date
Signed by: Will Jones	Will Jones	Vice President	1/27/2025
Signed by: Karina Woods	Karina Woods	Secretary	1/27/2025

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

COUNTY AUTHORIZED SIGNATURE:

Signature	Name	Title	Date
DocuSigned by: Christina Rojas	Christina Rojas	Deputy Purchasing Agent	1/28/2025

* If the contracting party is a corporation, (2) two signatures are required: one (1) signature by the Chairman of the Board, the President or any Vice President; and one (1) signature by the Secretary, any Assistant Secretary, the Chief Financial Officer or any Assistant Treasurer. The signature of one person alone is sufficient to bind a corporation, as long as he or she holds corporate offices in each of the two categories described above. For County purposes, proof of such dual office holding will be satisfied by having the individual sign the instrument twice, each time indicating his or her office that qualifies under the above described provision. In the alternative, a single corporate signature is acceptable when accompanied by a corporate resolution demonstrating the legal authority of the signee to bind the corporation.

ATTACHMENT A - SCOPE OF WORK

1. Scope of Work

The Scope of Work is described as follows.

2. General Information and Project Overview:

The County of Orange is comprised of 22 Departments and over 18,000 employees located throughout the County. The County's core businesses are public safety, public works, construction management, public health, environmental protection, regional planning, public assistance, social services, and aviation.

The County of Orange is seeking to partner with a qualified online marketplace company or companies that can provide a vast assortment of software products and cloud solutions. The County's intent is to obtain the most robust offerings while maximizing the quality and level of service. The Contractor is to provide software products and cloud solutions on an on-going or as needed basis.

3. Project Goals:

The purpose of this Contract is to provide County agencies and departments with cloud services & associated software products.

4. Project:

The County seeks to establish a contract with provider(s) that can offer Software, Cloud Services, Information Technology Consulting, Outsourcing, and related services that will meet technical requirements, provide user-friendly functionality, and meet County's business needs. This Contract shall include AWS or equivalent cloud computing services (Both US Government Cloud and Commercial Cloud Services to be made available based on business requirements).

The County anticipates continual releases of cloud services not specified in the Contract due to technological advances.

5. Contractor's Responsibilities:

1. Contractor shall hold mid-level tier partner status or above and be an authorized reseller for AWS or equivalent cloud computing services.

2. Contractor to provide example of cost reporting dashboard, or invoice which will be shared with County of Orange for billing purposes.

3. Confirmation County of Orange will have the ability to access AWS or equivalent Cost Explorer / "vendor cost tools" to review cloud consumption, and available savings plans.

4. Contractor to provide confirmation of Master Service Agreement with AWS/vendor or equivalent for Professional Services which can be made available.

5. Make available the option to obtain Software quotes or procure through vendor marketplace where additional discounts may be available.

6. Contract Usage:

Agencies/departments utilizing this Contract will submit a Scope of Service or Scope of Work and request a quote/proposal from Contractor. Services to Agencies/Departments will be "project specific" or at on an as-needed basis.

Project specific means that Contractor shall propose the number of hours or a fixed fee required to provide needed services. County Agencies/Departments will provide detailed information including, but not limited to, the type of system to be serviced, frequency of services to be performed, system location, whether parts must be included in the quote/proposal or will be reimbursed, name of requester and their Department, work site address, Contractor License Number if applicable, and any other relevant information in their scope of services for the required project and/or multiple projects. The requesting Agency/Department will review and express acceptance of the quote/proposal in writing. Agency/Department will issue their Subordinate Contract prior to commencement of services.

Agencies/Departments must allow a minimum of five (5) Business Days (Monday through Friday) for Contractors to respond to their quote/proposal.

Agency/Department Subordinate Contracts may require Board of Supervisor's approval in accordance with County's Procurement Policy.

Emergency Calls must be clearly identified and communicated to Contractor if a response is required in less than five (5) Business Days.

7. ADDITIONAL WORK CLAUSE FOR APPLICABLE SERVICE CONTRACTS:

A. **Additional Work:**

1. Upon County request, Contractor shall submit supplemental proposals for Additional Work not called for under the Scope of Work of this Contract. Contractor must obtain County Project Manager's written approval prior to commencing any additional work.
2. County reserves the right to obtain supplemental proposals from, and use, alternate sources for completion of the additional work and to utilize the data provided under this Contract to obtain necessary services.
3. If County authorizes work by an alternate source, Contractor may be relieved of responsibilities pertaining to the equipment affected by the project while work is being performed and during the subsequent warranty period.
4. Contractor shall continue to provide services to all areas not affected by work provided by alternate sources.
5. Upon completion of any additional work, whether by Contractor or an alternative source, County's Project Manager or designee and Contractor will inspect the finished product at no additional cost to County. Upon mutual acceptance of the additional work, Contractor shall again be responsible for all services originally covered under this Contract and the work performed under this section.

8. Miscellaneous Clause:

A. Miscellaneous commodities may be obtained at County's request. Contractor shall provide a written quote and obtain authorized County approval. Contractor under no circumstance shall provide any commodities without prior written authorized County approval. Additional delivery locations may be added or deleted at any time with no penalty to County. Miscellaneous item purchases shall not exceed $5,000.00, per item, including tax and other expenses, except when ordering the same items multiple times. Total order amount shall not exceed $25,000.00.

B. County may elect to accept substitute like commodities, commodities of equal or better quality and/or brand, costing equal or less than the original contracted commodities as set forth in this Contract with written authorized County approval. Substitute like commodities that cost more will require prior authorized approval from County before any substitution will take place.

ATTACHMENT B - PAYMENT AND COMPENSATION

1. **Compensation:** This is a usage Contract between County and Contractor for Service Description as set forth in Attachment A, "Scope of Work".

   Contractor agrees to accept the specified compensation as set forth in this Contract as full payment 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 Contractor of all its duties and obligations hereunder. Contractor shall only be compensated as set forth herein for work performed in accordance with the Scope of Work. **County shall have no obligation to pay any sum in excess of the fixed rates specified herein unless authorized by amendment in accordance with Articles "Changes" and "Amendments" of County Contract Terms and Conditions, which may require approval by the County Board of Supervisors.**

2. **Fees and Charges:** County will pay the fees and charges in accordance with the provisions of this Contract. Payment shall be as follows:

   Contractor will provide County Departments with a quote/proposal for project specific On-Line Marketplace Software and Cloud Services as outlined in Attachment A, Scope of Work. Contractor will provide quote/proposal at the minimum percentage discount listed below in Paragraph A for each of the AWS services required. If further savings, promotions or optimizations are available, the County expects to receive the best available rate on an ongoing basis. The minimum percentage discount off will remain constant during the duration of the Contract. It is understood that even though the Contract is for a minimum percentage discount off Contractor's published list price, deeper discounts may be applied.

   Contractor's quote/proposal must include the published list price at the time and date order was placed (referencing print-out from Contractor's website with date and time printed included). That quote/proposal shall be attached to the Delivery Order or Subordinate Contract issued against the RCA and included with the invoice that will be submitted for payment. Invoices submitted must include the published list price at the time of quote/proposal for software and/or services, the minimum percent discount applied and the total discounted price, including any miscellaneous items ordered in accordance with Attachment A, Paragraph 8. Miscellaneous Clause.

   A. Pricing and Minimum Percentage Discount off Amazon Web Services:

   Pricing Calculator for AWS Cloud Services (will generate list prices at time of each estimate):
   https://calculator.aws/#/?ch=cta&cta=lower-pricing-calc

Equipment/Goods By Line	Description	Service Category	Discount (%)
Amazon Web Services, LLC	Amazon Web Services	All	3%
Amazon Web Services, LLC	Support Services	Support	3%

Additional Links for reference:

Amazon Support Plan Pricing:
AWS Support Plan Pricing: https://aws.amazon.com/premiumsupport/pricing/

Amazon Marketplace:
AWS Marketplace: https://aws.amazon.com/marketplace

Additional Work: Any additional services not listed in the Contract must be approved by County's Project Manager or designee in accordance with Attachment "A", Section 9, item 9.6. Approval by the Board of Supervisors is required for all service contract where for any year of the contract, the annual value to any one contractor exceeds $200,000.

Approval by the Board of Supervisors is required for all service contracts where the total contract value exceeds or is anticipated to exceed $1,000,000 when all contract years are taken into consideration for multi-year contracts.

3. Price Increase/Decreases:

No price increases will be considered during the first year/term of the Contract. County requires documented proof of cost increases on Contracts prior to any price adjustment. A minimum of 30-days advance notice in writing is required for consideration of such adjustment. No retroactive price adjustments will be considered. All price decreases will automatically be extended to County of Orange. County may enforce, negotiate, or cancel escalating price Contracts or take any other action it deems appropriate, as it sees fit. The net dollar amount of profit will remain firm during the period of Contract. Adjustments increasing Contractor's profit will not be allowed.

4. Firm Discount and Pricing Structure:

Contractor guarantees that prices quoted are equal to or less than prices quoted to any other local, State or Federal government entity for services of equal or lesser scope. Contractor agrees that no price increases shall be passed along to County during the term of this Contract not otherwise specified and provided for within this Contract.

5. Contractor's Expense:

Contractor will be responsible for all costs related to photo copying, telephone communications and fax communications while on County sites during the performance of work and services under this Contract.

6. Payment Terms – Payment in Arrears:

Invoices are to be submitted in arrears to the user agency/department to the ship-to address, unless otherwise directed in this Contract. Contractor shall reference Contract number on invoice. Payment will be net 30 days after receipt of an invoice in a format acceptable to County of Orange and verified and approved by the agency/department and subject to routine processing requirements. The responsibility for providing an acceptable invoice rests with Contractor.

Billing shall cover services and/or goods not previously invoiced. Contractor shall reimburse County of Orange for any monies paid to Contractor for goods or services not provided or when goods or

services do not meet 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. Taxpayer ID Number:

Contractor shall include its taxpayer ID number on all invoices submitted to County for payment to ensure compliance with IRS requirements and to expedite payment processing.

8. Payment – Invoicing Instructions:

Payment – Invoicing Instructions: The Contractor will provide an invoice on the Contractor's letterhead for goods delivered and/or services rendered. In the case of goods, the Contractor will leave an invoice with each delivery. Each invoice will have a number and will include the following information:

a. Contractor's name and address

b. Contractor's remittance address, if different from "A" above

c. Contractor's Taxpayer ID Number

d. Name of County Agency/Department

e. Delivery/Service address

f. Contract TBD

g. Requisition TBD

h. Agency/Department's Account Number

i. Date of order

j. Product/Service description, quantity, and prices

k. Sales tax, if applicable

l. Freight/Delivery Charges, if applicable

m. Total

n. Quote/Proposal with published list price at the time order was placed for software and/or services, the minimum percent discount and the total discounted price, including any miscellaneous items ordered in accordance with Attachment A, Paragraph 8. Miscellaneous Clause.

Invoices and support documentation are to be forwarded to:

Contractor shall issue and send invoices according to each Department's instructions/requirements for each Subordinate Contract issued off this RCA. Adjustments increasing the Contractor's profit will not be allowed.

9. Payment (Electronic Funds Transfer (EFT):

County of Orange offers contractors the option of receiving payment directly to their bank account via an Electronic Fund Transfer (EFT) process in lieu of a check payment. Payment made via EFT will also receive an Electronic Remittance Advice with the payment details via e-mail. An e-mail address will need to be provided to The County of Orange via an EFT Authorization Form. To request a form, please contact the agency/department Procurement Buyer listed in Contract. Upon completion of the form, please mail, fax or email to the address or phone listed on the form.

All contractors who contract with the County of Orange ("County") shall work cooperatively to assist County in achieving the objectives and abide by the applicable terms under these Guidelines for all Controls one (1) thru six (6) below at all times during the term of its contract with County.

1 ASSET MANAGEMENT

Asset management establishes an organization's inventory of fixed and controlled assets and defines how these assets are managed during their lifecycle to ensure sustained productivity in support of the organization's critical services. An event that disrupts an asset can inhibit the organization from achieving its mission. An asset management program helps identify appropriate strategies that shall allow the assets to maintain productivity during disruptive events. There are four broad categories of assets: people, information, technology, and facilities.

The Cybersecurity Program strives to achieve and maintain appropriate protection of IT assets. Loss of accountability of IT assets could result in a compromise or breach of IT systems and/or a compromise or breach of sensitive or privacy data.

1.1 GOALS AND OBJECTIVES

1.1.1 Services are identified and prioritized.

1.1.2 Assets are inventoried, and the authority and responsibility for these assets is established.

1.1.3 The relationship between assets and the services they support is established.

1.1.4 The asset inventory is managed.

1.1.5 Access to assets is managed.

1.1.6 Information assets are categorized and managed to ensure the sustainment and protection of the critical service.

1.1.7 Facility assets supporting the critical service are prioritized and managed.

1.2 ASSET MANAGEMENT POLICY STATEMENTS

1.2.1 Services Inventory

1.2.1.1 Departments and/or contractors shall maintain an inventory of its services. This listing shall be used by the department and/or contractors to assist with its risk management analysis.

1.2.2 Asset Inventory – Information

1.2.2.1 All information that is created or used within the County's trusted environment in support of County business activities shall be considered the property of the County. All County property shall be used in compliance with this guideline.

1.2.2.2 County information is a valuable asset and shall be protected from unauthorized disclosure, modification, or destruction. Prudent information security standards and practices shall be implemented to ensure that the integrity, confidentiality, and availability of County information are not compromised. All County information shall be protected from the time of its creation through its useful life and authorized disposal.

1.2.2.3 Departments and/or contractors shall establish internal procedures for the secure handling

and storage of all electronically maintained County information that is owned or controlled by the department.

1.2.3 Asset Inventory - Technology (Devices, Software)

1.2.3.1 Departments and/or contractors shall maintain an inventory of all department and/or contractors managed devices that connect to County network resources or processes, stores, or transmits County data including but not limited to:

- Desktop computers,
- Laptop Computers,
- Tablets (iPads and Android devices),
- Mobile Phones (basic cell phones),
- Smart Phones (iPhones, Blackberry, Windows Phones and Android Phones),
- Servers,
- Storage devices,
- Network switches,
- Routers,
- Firewalls,
- Security Appliances,
- Internet of Things (IoT) devices,
- Printers,
- Scanners,
- Kiosks and Thin clients,
- Mainframe Hardware, and
- VoIP Phones.

1.2.3.2 Asset inventory shall map assets to the services they support.

1.2.3.3 Departments and/or contractors shall adopt a standard naming convention for devices (naming convention to be utilized as devices are serviced or purchased).

1.2.3.4 Each department and/or contractor shall ensure that all software used on County systems and in the execution of County business shall be used legally and in compliance with licensing agreements.

1.2.4 Asset Inventory - Facilities

1.2.4.1 Departments and/or contractors shall maintain an inventory of its facilities. This listing shall be used by the department and/or contractor to assist with its risk management analysis.

1.2.4.2 Departments and/or contractors shall identify the facilities used by its critical services.

1.2.5 Access Controls

1.2.5.1 Departments and/or contractors shall establish a procedure that ensures only users with legitimate business needs to access County IT resources are provided with user accounts.

1.2.5.2 Access to County information systems and information systems data shall be based on each user's access privileges. Access controls shall ensure that even legitimate users cannot access stored information unless they are authorized to do so. Access control should start by denying access to everything, and then explicitly granting access according to the "need to know" principle.

1.2.5.3 Access to County information and County information assets should be based on the principle

of “least privilege,” that is, grant no user greater access privileges to the information or assets than County responsibilities demand.

1.2.5.4 The owner of each County system, or their designee, provides written authorization for all internal and external user access.

1.2.5.5 All access to internal County computer systems shall be controlled by an authentication method involving a minimum of a user identifier (“ID”) and password combination that provides verification of the user’s identity.

1.2.5.6 All County workforce members, including contractors, are to be assigned a unique user ID to access the network as applicable.

1.2.5.7 A user account shall be explicitly assigned to a single, named individual. No group or shared computer accounts are permissible except when necessary and warranted due to legitimate business needs. Such need shall be documented prior to account creation and accounts activated only when necessary.

1.2.5.8 User accounts shall not be shared with others including, but not limited to, someone whose access has been denied or terminated.

1.2.5.9 Departments and/or contractors shall conduct regular reviews of the registered users’ access level privileges. System owners shall provide user listings to departments for confirmation of user’s access privileges.

1.2.6 Asset Sanitation/Disposal

1.2.6.1 Unless approved by County management, no County computer equipment shall be removed from the premises.

1.2.6.2 Prior to re-deployment, storage media shall be appropriately cleansed to prevent unauthorized exposure of data.

1.2.6.3 Surplus, donation, disposal or destruction of equipment containing storage media shall be appropriately disposed according to the terms of the equipment disposal services contract.

1.2.6.4 Sanitization methods for media containing County information shall be in accordance with NSA (National Security Agency) standards (for example, clearing, purging, or destroying).

1.2.6.5 Disposal of equipment shall be done in accordance with all applicable County, state or federal surplus property and environmental disposal laws, regulations or policies.

2 CONTROLS MANAGEMENT

The Controls Management domain focuses on the processes by which an organization plans, defines, analyzes, and assesses the controls that are implemented internally. This process helps the organization ensure the controls management objectives are satisfied.

This domain focuses on the resilience controls that allow an organization to operate during a time of stress. These resilience controls are implemented in the organization at all levels and require various levels of management and staff to plan, define, analyze, and assess.

2.1 GOALS AND OBJECTIVES

2.1.1 Control objectives are established.

2.1.2 Controls are implemented.

2.1.3 Control designs are analyzed to ensure they satisfy control objectives.

2.1.4 Internal control system is assessed to ensure control objectives are met.

2.2 CONTROL MANAGEMENT POLICY STATEMENTS

2.2.1 Physical and Environmental Security

2.2.1.1 Procedures and facility hardening measures shall be adopted to prevent attempts at and detection of unauthorized access or damage to facilities that contain County information systems and/or processing facilities.

2.2.1.2 Restricted areas within facilities that house sensitive or critical County information systems shall, at a minimum, utilize physical access controls designed to permit access by authorized personnel only.

2.2.1.3 Physical protection measures against damage from external and environmental threats shall be implemented by all departments as appropriate.

2.2.1.4 Access to any office, computer room, or work area that contains sensitive information shall be physically restricted from unauthorized access.

2.2.1.5 Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. An example of this would be separating the two areas by a badge-only accessible door.

2.2.1.6 Continuity of power shall be provided to maintain the availability of critical equipment and information systems.

2.2.1.7 Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage. Different, yet appropriate methods shall be utilized for internal and external cabling.

2.2.1.8 Equipment shall be properly maintained to ensure its continued availability and integrity.

2.2.1.9 All shared IT infrastructure by more than one department shall meet countywide security policy for facility standards, availability, access, data & network security.

2.2.2 Network Segmentation

NOTE: This section is applicable to Departments and/or contractors that manage their own network devices.

2.2.2.1 Segment (e.g., VLANs) the network into multiple, separate zones (based on trust levels of the information stored/transmitted) to provide more granular control of system access and additional intranet boundary defenses. Whenever information flows over a network of lower trust level, the information shall be encrypted.

2.2.2.2 Segment the network into multiple, separate zones based on the devices (servers, workstations, mobile devices, printers, etc.) connected to the network.

2.2.2.3 Create separate network segments (e.g., VLANs) for BYOD (“bring your own device”) systems or other untrusted devices.

2.2.2.4 The network infrastructure shall be managed across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

2.2.3 Mobile Computing Devices

To ensure that Mobile Computing Devices (“MCDs”) do not introduce threats into systems that process or store County information, departments’ and/or contractors’ management shall:

2.2.3.1 Establish and manage a process for authorizing, issuing and tracking the use of MCDs.

2.2.3.2 Permit only authorized MCDs to connect to County information assets or networks that store, process, transmit, or connects to County information and information assets.

2.2.3.3 Implement applicable access control requirements in accordance with this guideline, such as the enforcement of a system or device lockout after 15 minutes of inactivity requiring re-entering of a password to unlock.

2.2.3.4 Install an encryption algorithm that meets or exceeds industry recommended encryption standard for any MCD that will be used to store County information.

2.2.3.5 Ensure that MCDs are configured to restrict the user from circumventing the authentication process.

2.2.3.6 Provide security awareness training to County and/or contractor employees that informs MCD users regarding MCD restrictions.

2.2.3.7 Label MCDs with County address and/or phone number so that the device can be returned to the County if recovered.

2.2.3.8 The installation of any software, executable, or other file to any County computing device is prohibited if that software, executable, or other file downloaded by, is owned by, or was purchased by an employee or contractor with his or her own funds unless approved by the department.

2.2.4 Personally Owned Devices

Personal computing devices include, but are not limited to, removable media such as thumb or USB drives, external hard drives, laptop or desktop computers, cellular phones, or personal digital assistants (“PDA's”) owned by or purchased by employees, contract personnel, or other non-County users.

2.2.4.1 The connection of any computing device not owned by the County to a County network (except the Public Wi-Fi provided for public use) or computing device is prohibited unless previously approved.

2.2.4.2 The County authorizes the use of personal devices to access resources that do not traverse the County network directly. Such resources include County’s SaaS applications. Access to some agency specific applications, e.g., applications that are subject to compliance regulations, may require prior approval of the County CISO and the associated Department Head.

2.2.4.3 The County will respect the privacy of a user’s voluntary use of a personally owned devices to access County IT resources.

2.2.4.4 The County will only request access to the personally owned device in order to implement security controls, to respond to litigation hold (aka: e-discovery) requests arising out of administrative, civil, or criminal directives, Public Record Act requests, and subpoenas (or as otherwise required or permitted by applicable state or federal laws). Such access will be performed by an authorized technician or designee using a legitimate software process.

2.2.5 Logon Banners and Warning Notices

2.2.5.1 At the time of network login, the user shall be presented with a login banner.

2.2.5.2 All computer systems that contain or access County information shall display warning banners informing potential users of conditions of use consistent with state and federal laws.

2.2.5.3 Warning banners shall remain on the screen until the user takes explicit actions to log on to the information system.

2.2.5.4 The banner message shall be placed at the user authentication point for every computer

system that contains or accesses County information. The banner message may be placed on an initial logon screen in situations where the logon provides access to multiple computer systems.

2.2.5.5 At a minimum, banner messages shall provide appropriate privacy and security information and shall contain information informing potential users that:

- User is accessing a government information system for conditions of use consistent with state and federal information security and privacy protection laws.
- System usage may be monitored, recorded, and subject to audit.
- Unauthorized use of the system is prohibited and subject to criminal and civil penalties.
- Use of the system indicates consent to monitoring and recording.

2.2.6 Authentication

2.2.6.1 Authenticate user identities at initial connection to County resources.

2.2.6.2 Authentication mechanisms shall be appropriate to the sensitivity of the information contained.

2.2.6.3 Users shall not receive detailed feedback from the authenticating system on failed logon attempts.

2.2.7 Passwords

2.2.7.1 County approved password standards and/or guidelines shall be applied to access County systems. These standards extend to mobile devices and personally owned devices used for work.

2.2.7.2 Passwords are a primary means to control access to systems and shall therefore be selected, used, and managed to protect against unauthorized discovery or usage. Passwords shall satisfy the following complexity rule:

- Passwords will contain a minimum of one (1) upper case letter
- Passwords will contain a minimum of one (1) lower case letter
- Passwords will contain a minimum of one (1) number: 1- 0
- Passwords will contain a minimum of one (1) special character: !,@,#,$,%,^,&,*,(,)
- Password characters will not be sequential (Do not use: ABCD , This is ok: ACDB)
- Passwords characters will not be repeated in a row (Do not use: P@$$S. This is ok: P@S)
- COMPLEX PASSWORD EXAMPLE: P@$SWoRd13
- Passphrases example: The$kyIsBlue2day
- Passwords cannot contain the user's full name or network login

2.2.7.3 Passwords shall have a minimum length of twelve (12) characters.

2.2.7.4 Passwords shall not be reused for twelve (12) iterations.

2.2.7.5 Departments and/or contractors shall require users to change their passwords periodically (e.g., every 90 days at the maximum). Changing passwords more often than 90 days is encouraged.

2.2.7.6 Network and application systems shall be configured to enforce automatic expiration of passwords at regular intervals (e.g., every 90 days at the maximum) when the technology is feasible or available.

2.2.7.7 Newly created accounts shall be assigned a randomly generated password prior to account information being provided to the user.

2.2.7.8 No user shall give his or her password to another person under any circumstances.

Workforce members who suspect that their password has become known by another person shall change their password immediately and report their suspicion to management.

2.2.7.9 Users who have lost or forgotten their passwords shall make any password reset requests themselves without using a proxy (e.g., another County employee) unless approved by management. Prior to processing password change requests, the requester shall be authenticated to the user account in question. (e.g., Verification with user's supervisor or the use of passphrases can be used for this authentication process.) New passwords shall be provided directly and only to the user in question.

2.2.7.10 When technologically feasible, a new or reset password shall be set to expire on its initial use at log on so that the user is required to change the provided password to one known only to them.

2.2.7.11 All passwords are to be treated as sensitive information.

2.2.7.12 User Accounts shall be locked after five (5) consecutive invalid logon attempts within a 24-hour period. The lockout duration shall be at least 30 minutes or until a system administrator enables the user ID after investigation. These features shall be configured as indicated when the technology is feasible or available.

2.2.7.13 All systems containing sensitive information shall not allow users to have multiple concurrent sessions on the same system when the technology is feasible or available.

2.2.8 Inactivity Timeout and Restricted Connection Times

2.2.8.1 Automatic lockouts for system devices, including workstations and mobile computing devices, after no more than 15 minutes of inactivity.

2.2.8.2 Automated screen lockouts shall be used wherever possible using a set time increment (e.g., 15 minutes of non-activity). In situations where it is not possible to automate a lockout, operational procedures shall be implemented to instruct users to lock the terminal or equipment so that unauthorized individuals cannot make use of the system. Once logged on, workforce members shall not leave their computer unattended or available for someone else to use.

2.2.8.3 When deemed necessary, user logins and data communications may be restricted by time and date configurations that limit when connections shall be accepted.

2.2.9 Account Monitoring

2.2.9.1 Access to a County network and its resources shall be strictly controlled, managed, and reviewed to ensure only authorized users gain access based on the privileges granted. (e.g., Kiosks provide physical and public access to County networks. These shall be secured to ensure County resources are not accessed by unauthorized users.)

2.2.9.2 The control mechanisms for all types of access to County IT resources by contractors and customers are to be documented.

2.2.9.3 Monitor account usage to determine dormant accounts that have not been used for a given period, such as 45 days, notifying the user or user's manager of the dormancy.

2.2.9.4 After a longer period, such as 60 days, the account shall be disabled by the system when the technology is feasible or available.

2.2.9.5 On a periodic basis, such as quarterly or at least annually, departments shall require that managers match active employees and contractors with each account belonging to their managed staff. Security or system administrators shall then determine whether to disable accounts that are not assigned to active employees or contractors.

2.2.10 Administrative Privileges

2.2.10.1 Systems Administrators shall use separate administrative accounts, which are different

from their end user account (required to have an individual end user account), to conduct system administration tasks.

2.2.10.2 Administrative accounts shall only be granted to individuals who have a job requirement to conduct systems administration tasks.

2.2.10.3 Administrative accounts shall be requested in writing and must be approved by the Department Head or designated representative using the County Security Review and Approval Process.

2.2.10.4 Systems Administrator accounts that access County enterprise-wide systems or have enterprise-wide impact shall be approved by the CISO using the County Security Review and Approval Process.

2.2.10.5 Systems Administrators shall use separate administrative accounts to manage Mobile Device Management (MDM) platforms but may use the local user's credentials when configuring a mobile phone or tablet device.

2.2.10.6 All passwords for privileged system-level accounts (e.g., root, enable, OS admin, application administration accounts, etc.) shall comply with Section 2.2.7.2.

2.2.11 Remote Access

2.2.11.1 Departments and/or contractors shall take appropriate steps, including the implementation of appropriate encryption, user authentication, and virus protection measures, to mitigate security risks associated with allowing users to use remote access or mobile computing methods to access County information systems.

2.2.11.2 Remote access privileges shall be granted to County workforce and contractors only for legitimate business needs and with the specific approval of department management.

2.2.11.3 All remote access implementations that utilize the County's trusted network environment and that have not been previously deployed within the County shall be submitted to and reviewed by the County. A memorandum of understanding (MOU) shall be utilized for this submittal and review process. This is required for any Suppliers utilizing remote access to conduct maintenance.

2.2.11.4 Remote sessions shall be terminated after 15 minutes of inactivity requiring the user to authenticate again to access County resources.

2.2.11.5 All remote access infrastructure shall include the capability to monitor and record a detailed audit trail of each remote access attempt.

2.2.11.6 All users of County networks and computer systems are prohibited from connecting and/or activating unauthorized dial-up or broadband modems on workstations, laptops, or other computing devices that are simultaneously connected to any County network.

2.2.11.7 Periodic assessments shall be performed to identify unauthorized remote connections. Results shall be used to address any vulnerabilities and prioritized according to criticality.

2.2.11.8 Users granted remote access to County IT infrastructure shall follow all additional policies, guidelines and standards related to authentication and authorization as if they were connected locally. For example, this applies when mapping to shared network drives.

2.2.11.9 Users attempting to use external remote access shall utilize a County-approved multi-factor authentication process.

2.2.11.10 All remote access implementations that involve non-County infrastructure shall be reviewed and approved by both the department and County. This approval shall be received prior to the start of such implementation.

2.2.11.11 Remote access privileges to County IT resources shall not be given to contractors and

customers unless department management determines that these individuals or organizations have a legitimate business need for such access. If such access is granted, it shall be limited to those privileges and conditions required for the performance of the specified work.

2.2.12 Wireless Access

2.2.12.1 Departments and/or contractors shall take appropriate steps, including the implementation of appropriate encryption, user authentication, device authentication and malware protection measures, to mitigate risks to the security of County data and information systems associated with the use of wireless network access technologies.

2.2.12.2 Only wireless systems that have been evaluated for security by both department management and the County shall be approved for connectivity to County networks.

2.2.12.3 County data that is transmitted over any wireless network shall be protected in accordance with the sensitivity of the information.

2.2.12.4 All access to County networks or resources via unapproved wireless communication technologies is prohibited. This includes wireless systems that may be brought into County facilities by visitors or guests. Employees, contractors, and customers are prohibited from connecting and/or activating wireless connections on any computing device that are simultaneously connected to any County network, either locally or remotely.

2.2.12.5 Each department and/or contractor shall make a regular, routine effort to ensure that unauthorized wireless networks, access points, and/or modems are not installed or configured within its IT environments. Any unauthorized connections described above shall be disabled immediately.

2.2.13 System and Network Operations Management

2.2.13.1 Operating procedures and responsibilities for all County information processing facilities shall be formally authorized, documented, and updated.

2.2.13.2 Departments and/or contractor shall establish controls to ensure the security of the information systems networks that they operate.

2.2.13.3 Operational system documentation for County information systems shall be protected from unauthorized access.

2.2.13.4 System utilities shall be available to only those users who have a business case for accessing the specific utility.

2.2.14 System Monitoring and Logging

2.2.14.1 Systems operational staff shall maintain appropriate log(s) of activities, exceptions and information security events involving County information systems and services.

2.2.14.2 Each department and/or contractor shall maintain a log of all faults involving County information systems and services.

2.2.14.3 Logs shall be protected from unauthorized access or modifications wherever they reside.

2.2.14.4 The clocks of all relevant information processing systems and attributable logs shall be synchronized with an agreed upon accurate time source such as an established Network Time Protocol (NTP) service.

2.2.14.5 Auditing and logging of user activity shall be implemented on all critical County systems that support user access capabilities.

2.2.14.6 Periodic log reviews of user access and privileges shall be performed in order to monitor access of sensitive information.

2.2.15 Malware Defenses

2.2.15.1 Departments shall implement endpoint security on computing devices connected to the County network. Endpoint security may include one or more of the following software: anti-virus, anti- spyware, personal firewall, host-based intrusion detection (IDS), network-based intrusion detection (IDS), intrusion prevention systems (IPS), and whitelisting and blacklisting of applications, web sites, and IP addresses.

2.2.15.2 Special features designed to filter out malicious software contained in either email messages or email attachments shall be implemented on all County email systems.

2.2.15.3 Where feasible, any computing device, including laptops and desktop PCs, that has been connected to a non-County infrastructure (including employee home networks) and subsequently used to connect to the County network shall be verified that it is free from viruses and other forms of malicious software prior to attaining connectivity to the County network.

2.2.16 Data Loss Prevention

2.2.16.1 Departments and/or contractors shall implement Data Loss Prevention (DLP) methods to reduce the risk of data breach related to sensitive information.

2.2.16.2 Departments and/or contractors shall deploy encryption software on mobile devices containing sensitive data.

2.2.17 Data Transfer

2.2.17.1 Agreements shall be implemented for the exchange of information between the County and other entities. As well as between departments.

2.2.17.2 County information accessed via electronic commerce shall have security controls implemented based on the assessed risk.

2.2.18 Encryption

2.2.18.1 The decision to use cryptographic controls and/or data encryption in an application shall be based on the level of risk of unauthorized access and the sensitivity of the data that is to be protected.

2.2.18.2 The decision to use cryptographic controls and/or data encryption on a hard drive or any removable media/device shall be based on the level of risk of unauthorized access and the sensitivity of the data that is to be protected.

2.2.18.3 Where appropriate, encryption shall be used to protect confidential application data that is transmitted over open, untrusted networks, such as the Internet.

2.2.18.4 When cryptographic controls are used, procedures addressing the following areas shall be established by each department:

2.2.18.5 Determination of the level of cryptographic controls

2.2.18.6 Key management/distribution steps and responsibilities

2.2.18.7 Encryption keys shall be exchanged only using secure methods of communication.

2.2.19 System Acquisition and Development

2.2.19.1 Departments and/or contractors shall identify all business applications that are used by their users in support of primary business functions. This includes all applications owned and/or managed by the department as well as other business applications that are used by the department but owned and/or managed by other County organizations. All business applications used by a department shall be documented in the department's IT security plan as well as their Business Impact Analysis (BIA) for criticality rating (RTO) and continuity purposes.

2.2.19.2 An application owner shall be designated for each internal department business application.

2.2.19.3 All access controls associated with business applications shall be commensurate with the highest level of data used within the application. These same access controls shall also adhere to the guidelines provided in Section 1.2.5: Access Controls.

2.2.19.4 Security requirements shall be incorporated into the evaluation process for all commercial software products that are intended to be used as the basis for a business application. The security requirements in question shall be based on requirements and standards specified in this guideline.

2.2.19.5 In situations where data needs to be isolated because there would be a conflict of interest data security shall be designed and implemented to ensure that isolation.

Business Requirements

2.2.19.6 The business requirements definition phase of system development shall contain a review to ensure that the system shall adhere to County information security standards.

System Files

2.2.19.7 Operating system files, application software and data shall be secured from unauthorized use or access.

2.2.19.8 Clear-text data that results from testing shall be handled, stored, and disposed of in the same manner and using the same procedures as are used for production data.

2.2.19.9 System tests shall be performed on data that is constructed specifically for that purpose.

2.2.19.10 System testing shall not be performed on operational data unless the necessary safeguards are in place.

2.2.19.11 A combination of technical, procedural and physical safeguards shall be used to protect application source code from unintentional or unauthorized modification or destruction. All County proprietary information, including source code, needs to be protected through appropriate role-based access controls. An example of this is a change control tool that records all changes to source code including new development, updates, and deletions, along with check-in and check-out information.

System Development & Maintenance

2.2.19.12 The development of software for use on County information systems shall have documented change control procedures in place to ensure proper versioning and implementation.

2.2.19.13 When preparing to upgrade any County information systems, including an operating system, on a production computing resource; the process of testing and approving the upgrade shall be completed in advance in order to minimize potential security risks and disruptions to the production environment.

2.2.19.14 Any outside suppliers used for maintenance that are visitors to the facility are to be escorted and monitored while performing maintenance to critical systems. This does not apply to contractors that are assigned to work at the facility.

2.2.19.15 Systems shall be hardened, and logs monitored to ensure the avoidance of the introduction and exploitation of malicious code.

2.2.19.16 All County workforce members, including contractors, shall not create, execute, forward, or introduce computer code designed to self-replicate, damage, or impede the performance of a computer's memory, storage, operating system, or application software.

2.2.19.17 In conjunction with other access control policies, any opportunity for information leakage shall be prevented through good system design practices.

2.2.19.18 Departments and/or contractors are responsible for managing outsourced software development related to department-owned IT systems.

System Requirements

Any system that processes or stores County Information shall:

2.2.19.19 Baseline configuration shall incorporate Principle of Least Privilege and Functionality.

2.2.19.20 Systems shall be deployed where feasible to utilize existing County authentication methods.

2.2.19.21 Session inactivity timeouts shall be implemented for all access into and from County networks.

2.2.19.22 All applications are to have access controls unless specifically designated as a public access resource.

2.2.19.23 Meet the password requirements defined in Section 2.2.7: Passwords.

2.2.19.24 Strictly control access enabling only privileged users or supervisors to override system controls or the capability of bypassing data validation or editing problems.

2.2.19.25 Monitor special privilege access, e.g., administration accounts.

2.2.19.26 Restrict authority to change master files to persons independent of the data processing function.

2.2.19.27 Have access control mechanisms to prevent unauthorized access or changes to data, especially, the server file systems that are connected to the Internet, even behind a firewall.

2.2.19.28 Be capable of routinely monitoring the access to automated systems containing County Information.

2.2.19.29 Log all modifications to the system files.

2.2.19.30 Limit access to system utility programs to necessary individuals with specific designation.

2.2.19.31 Maintain audit logs on a device separate from the system being monitored.

2.2.19.32 Delete or disable all default accounts.

2.2.19.33 Restrict access to server file-system controls to ensure that all changes such as direct write, write access to system areas and software or service changes shall be applied only through the appropriate change control process.

2.2.19.34 Restrict access to server-file-system controls that allow access to other users' files.

2.2.19.35 Ensure that servers containing user credentials shall be physically protected, hardened and monitored to prevent inappropriate use.

2.2.20 Procurement Controls

2.2.20.1 Breach notification requirements clause to be included in new or renewal contracts for systems containing sensitive information.

2.2.20.2 Contractor shall report to the County immediately or within 24 hours when contractor becomes aware of any potential or suspected data breach of contractor's or subcontractor's systems involving County's data.

2.2.20.3 Departments shall review all procurements and renewals for software and equipment (hosted/managed by the contractor) that transmits, stores, or processes sensitive information to

ensure that contractors are aware of and are in compliance with County's cybersecurity policies if applicable. Departments shall obtain documentation supporting the business partners, contractors, or consultants' compliance with County's cybersecurity policies such as:

- SOC 1 Type 2
- SOC 2 Type 2
- Security Certifications (ISO, PCI, etc.)
- FedRAMP certification
- Penetration Test Results

2.2.21 IT Services Provided to Public

2.2.21.1 Public access to County electronic information resources shall provide desired services in accordance with safeguards designed to protect County resources. All County electronic information resources are to be reviewed at least quarterly.

2.2.22 Removable Media

2.2.22.1 When no longer required, the contents of removable media shall be permanently destroyed or rendered unrecoverable in accordance with applicable department, County, state, or federal record disposal and/or retention requirement.

3 CONFIGURATION & CHANGE MANAGEMENT

Configuration and Change Management ("CCM") is the process of maintaining the integrity of hardware, software, firmware, and documentation related to the configuration and change management process. CCM is a continuous process of controlling and approving changes to information or technology assets or related infrastructure that support the critical services of an organization. This process includes the addition of new assets, changes to assets, and the elimination of assets.

Cybersecurity is an integral component to information systems from the onset of the project or acquisition through implementation of:

- Application and system security
- Configuration management
- Change control procedures
- Encryption and key management
- Software maintenance, including but not limited to, upgrades, antivirus, patching and malware detection response systems

As the complexity of information systems increases, the complexity of the processes used to create these systems also increases, as does the probability of accidental errors in configuration. The impact of these errors puts data and systems that may be critical to business operations at significant risk of failure that could cause the organization to lose business, suffer damage to its reputation, or close completely. Having a CCM process to protect against these risks is vital to the overall security posture of the organization.

3.1 GOALS AND OBJECTIVES

3.1.1 The lifecycle of assets is managed.

3.1.2 The integrity of technology and information assets is managed.

3.1.3 Asset configuration baselines are established.

3.2 CONFIGURATION & CHANGE MANAGEMENT POLICY STATEMENTS

3.2.1 Changes to all information processing facilities, systems, software, or procedures shall be strictly controlled according to formal change management procedures.

3.2.2 Changes impacting security appliances managed by the County (e.g., security architecture, security appliances, County firewall, Website listings, application listings, email gateway, administrative accounts) shall be reviewed by the County in accordance with the County Security Review and Approval Process.

3.2.3 Only authorized users shall make any changes to system and/or software configuration files.

3.2.4 Only authorized users shall download and/or install operating system software, service-related software (such as web server software), or other software applications on County computer systems/devices without prior written authorization from department IT management. This includes, but is not limited to, free software, computer games and peer-to-peer file sharing software.

3.2.5 Each department and/or contractor shall develop a formal change control procedure that outlines the process to be used for identifying, classifying, approving, implementing, testing, and documenting changes to its IT resources.

3.2.6 Each department and/or contractor shall conduct periodic audits designed to determine if unauthorized software has been installed on any of its computers.

3.2.7 As appropriate, segregation of duties shall be implemented by all County departments to ensure that no single person has control of multiple critical systems and the potential for misusing that control.

3.2.8 Production computing environments shall be separated from development and test computing environments to reduce the risk of one environment adversely affecting another.

3.2.9 System capacity requirements shall be monitored, and usage projected to ensure the continual availability of adequate processing power, bandwidth, and storage.

3.2.10 System acceptance criteria for all new information systems and system upgrades shall be defined, documented, and utilized to minimize risk of system failure.

4 VULNERABILITY MANAGEMENT

The Vulnerability Management domain focuses on the process by which organizations identify, analyze, and manage vulnerabilities in a critical service's operating environment.

4.1 GOALS AND OBJECTIVES

4.1.1 Preparation for vulnerability analysis and resolution activities is conducted.

4.1.2 A process for identifying and analyzing vulnerabilities is established and maintained.

4.1.3 Exposure to identified vulnerabilities is managed.

4.1.4 The root causes of vulnerabilities are addressed.

4.2 VULNERABILITY MANAGEMENT POLICY STATEMENTS

4.2.1 Departments and/or contractors shall develop and maintain a vulnerability management process as part of its Cybersecurity Program.

5 CYBERSECURITY INCIDENT MANAGEMENT

Information Security Incident Management establishes the policy to be used by each department and/or contractor in planning for, reporting on, and responding to computer security incidents. For these purposes an incident is defined as any irregular or adverse event that occurs on a County system or network. The goal of incident management is to mitigate the impact of a disruptive event. To accomplish this goal, an organization establishes processes that:

- detect and identify events
- triage and analyze events to determine whether an incident is underway
- respond and recover from an incident
- improve the organization's capabilities for responding to a future incident

This domain defines management controls for addressing cyber incidents. The controls provide a consistent and effective approach to Cyber Incident Response aligned with the County's Cyber Incident Response Plan, to include:

- Collection of evidence related to the cyber incident as appropriate
- Reporting procedures including any and all statutory reporting requirements
- Incident remediation
- Minimum logging procedures
- Annual testing of the plan

5.1 GOALS AND OBJECTIVES

5.1.1 A process for identifying, analyzing, responding to, and learning from incidents is established.

5.1.2 A process for detecting, reporting, triaging, and analyzing events is established.

5.1.3 Incidents are declared and analyzed.

5.1.4 A process for responding to and recovering from incidents is established.

5.1.5 Post-incident lessons learned are translated into improvement strategies.

5.2 CYBERSECURITY INCIDENT MANAGEMENT POLICY STATEMENTS

5.2.1 Cybersecurity incident management procedures shall be established within each department and/or contractor to ensure quick, orderly, and effective responses to security incidents. In the event a department has not established these procedures, the department may adopt the County's Cyber Incident Response Plan. The steps involved in managing a security incident are typically categorized into six stages:

5.2.2 System preparation

5.2.3 Problem identification

5.2.4 Problem containment

5.2.5 Problem eradication

5.2.6 Incident recovery

5.2.7 Lessons learned

5.2.8 The department shall act as the liaison between applicable parties during a cybersecurity incident. The department shall be the department's primary point of contact for all IT security issues.

5.2.9 A designated security contact for all cybersecurity incidents.

5.2.10 Departments and/or contractors shall conduct periodic (at least annually) cybersecurity incident

scenario sessions for personnel associated with the cybersecurity incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the cybersecurity incident handling team.

5.2.11 Departments and/or contractors shall develop and document procedures for reporting cybersecurity incidents. For example, all employees, contractors, and customers of County information systems shall be required to note and report any observed or suspected security weaknesses in systems to management. In the event a department has not established these procedures, the department may adopt the County's Cyber Incident Response Plan.

5.2.12 Each department and/or contractor shall familiarize its employees on the use of its cybersecurity incident reporting procedures.

5.2.13 Contact with local authorities, including law enforcement, shall be conducted through an organized, repeatable process that is both well documented and communicated.

5.2.14 Contact with special interest groups, including media and labor relations, shall be conducted through an organized, repeatable process that is both well documented and communicated.

5.2.15 Where a follow-up action against an entity after a cybersecurity incident shall involve civil or criminal legal action, evidence shall be collected, retained, and presented to conform to the rules for evidence as demanded by the relevant jurisdiction(s). At the Department's discretion, they may obtain the services of qualified external professionals to complete these tasks.

5.2.16 Departments and/or contractors shall report cybersecurity incidents to the County pursuant to the Contract.

6 SERVICE CONTINUITY MANAGEMENT

Service continuity planning is one of the more important aspects of resilience management because it provides a process for preparing for and responding to disruptive events, whether natural or man-made. Operational disruptions may occur regularly and can scale from so small that the impact is essentially negligible to so large that they could prevent an organization from achieving its mission. Services that are most important to an organization's ability to meet its mission are considered essential and are focused on first when responding to disruptions. The process of identifying and prioritizing services and the assets that support them is foundational to service continuity.

Service continuity planning provides the organization with predefined procedures for sustaining essential operations in varying adverse conditions, from minor interruptions to large-scale incidents. For example, a power interruption or failure of an IT component may necessitate manual workaround procedures during repairs. A data center outage or loss of a business or facility housing essential services may require the organization to recover business or IT operations at an alternate location.

The process of assessing, prioritizing, planning and responding to, and improving plans to address disruptive events is known as service continuity. The goal of service continuity is to mitigate the impact of disruptive events by utilizing tested or exercised plans that facilitate predictable and consistent continuity of essential services.

This domain defines requirements to document, implement and annually test plans, including the testing of all appropriate cybersecurity provisions, to minimize impact to systems or processes from the effects of major failures of information systems or disasters via adoption and annual testing of:

- Business Continuity Plan
- Disaster Recovery Plan
- Cyber Incident Response Plan

Business Continuity is intended to counteract interruptions in business activities and to protect critical business processes from the effects of significant disruptions. Disaster Recovery provides for the restoration of critical County assets, including IT infrastructure and systems, staff, and facilities.

6.1 GOALS AND OBJECTIVES

6.1.1 Service continuity plans for high-value services are developed.

6.1.2 Service continuity plans are reviewed to resolve conflicts between plans.

6.1.3 Service continuity plans are tested to ensure they meet their stated objectives.

6.1.4 Service continuity plans are tested, executed, and reviewed.

6.2 SERVICE CONTINUITY MANAGEMENT POLICY STATEMENTS

6.2.1 Backups of all essential electronically maintained County business data and system configurations shall be routinely created and properly stored to ensure prompt restoration.

6.2.2 Each department and/or contractor shall implement and document a backup approach for ensuring the availability of critical application databases, system configuration files, and/or any other electronic information critical to maintaining normal business operations within the department.

6.2.3 The frequency and extent of backups shall be in accordance with the importance of the information and the acceptable risk as determined by each department.

6.2.4 Departments and/or contractors shall ensure that locations where backup media are stored are safe, secure, and protected from environmental hazards. Access to backup media shall be commensurate with the highest level of information stored and physical access controls shall meet or exceed the physical access controls of the data's source systems.

6.2.5 Backup media shall be labeled and handled in accordance with the highest sensitivity level of the information stored on the media.

6.2.6 Departments and/or contractors shall define and periodically test a formal procedure designed to verify the success of the backup process.

6.2.7 Restoration from backups shall be tested initially once the process is in place and periodically afterwards. Confirmation of business functionality after restoration shall also be tested in conjunction with the backup procedure test.

6.2.8 Departments and/or contractors shall retain backup information only as long as needed to carry out the purpose for which the data was collected, or for the minimum period required by law.

6.2.9 Alternate storage facilities shall be used to ensure confidentiality, integrity and availability of all County systems.

6.2.10 Each department and/or contractor shall develop, periodically update, and regularly test business continuity and disaster recovery plans.

6.2.11 Departments and/or contractors shall review and update their Risk Assessments (RAs) and Business Impact Analyses (BIAs) as necessary, determined by department management (annually is recommended). RAs include department identification of risks that can cause interruptions to business processes along with the probability and impact of such interruptions and the consequences to information security. A BIA establishes the list of processes and systems that the department has deemed critical after performing a risk analysis.

6.2.12 Continuity plans shall be developed and implemented to provide for continuity of business operations in the event that critical IT assets become unavailable. Plans shall provide for the availability of information at the required level and within the established Recovery Time Objective (RTO) and their location, as alternate facilities shall be used to maintain continuity.

6.2.13 Each department and/or contractor shall maintain a comprehensive plan document containing its

business continuity plans. Plans shall be consistent, address information security requirements, and identify priorities for testing and maintenance.

6.2.14 Each department and/or contractor shall define failure prevention protocols to maintain confidentiality, integrity and availability. Departments and/or contractors shall automate failover procedures where applicable and maintain adequate (predictable) levels of ancillary components to meet this provision.

ATTACHMENT D
BUSINESS ASSOCIATE CONTRACT

A. GENERAL PROVISIONS AND RECITALS

1. The Parties agree that the terms used, but not otherwise defined below in Paragraph B, 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 regulations promulgated thereunder by the U.S. Department of Health and Human Services (DHHS) ("the HIPAA regulations") (45 CFR Parts 160, 162 and 164) 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 Contractor 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, the Agreement that are described in the definition of "Business Associate" in 45 CFR § 160.103.

3. The County wishes to disclose to Contractor certain information pursuant to the terms of the Agreement, some of which may constitute Protected Health Information ("PHI"), as defined below in Subparagraph B.10, to be used or disclosed in the course of providing services and activities pursuant to, and as set forth, in the Agreement.

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 the Agreement 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 Subparagraphs B.9 and B.14, apply to the Contractor in the same manner as they apply to a covered entity (County). Contractor agrees therefore to be in compliance at all times with the terms of this Business Associate Contract and the applicable standards, implementation specifications, and requirements of the Privacy and the Security rules, as they may exist now or be hereafter amended, with respect to PHI and electronic PHI created, received, maintained, transmitted, used, or disclosed pursuant to the Agreement.

B. DEFINITIONS

1. "Administrative Safeguards" are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect

electronic PHI and to manage the conduct of Contractor's workforce in relation to the protection of that information.

2. "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.

a. Breach excludes:

i. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of Contractor 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.

ii. Any inadvertent disclosure by a person who is authorized to access PHI at Contractor to another person authorized to access PHI at the Contractor, 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.

iii. A disclosure of PHI where Contractor 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.

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

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

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

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

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

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

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

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

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

7. "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).

8. "Physical Safeguards" are physical measures, policies, and procedures to protect

CONTRACTOR's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

9. "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.

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

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

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

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

14. "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.

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

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

17. "Unsecured PHI" or "PHI that is unsecured" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of Health and Human Services in the guidance issued on the HHS Web site –
http://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html .

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

C. OBLIGATIONS AND ACTIVITIES OF CONTRACTOR AS BUSINESS ASSOCIATE:

1. Contractor agrees not to use or further disclose PHI County discloses to Contractor other than as permitted or required by this Business Associate Contract or as required by law.

2. Contractor agrees to use appropriate safeguards, as provided for in this Business Associate Contract and the Agreement, to prevent use or disclosure of PHI County discloses to Contractor or Contractor creates, receives, maintains, or transmits on behalf of County other than as provided for by this Business Associate Contract.

3. Contractor agrees to comply with the HIPAA Security Rule at Subpart C of 45 CFR Part 164 with respect to electronic PHI County discloses to Contractor or Contractor creates, receives,

maintains, or transmits on behalf of County.

4. Contractor agrees to mitigate, to the extent practicable, any harmful effect that is known to Contractor of a Use or Disclosure of PHI by Contractor in violation of the requirements of this Business Associate Contract.

5. Contractor agrees to report to County immediately any Use or Disclosure of PHI not provided for by this Business Associate Contract of which Contractor becomes aware. Contractor must report Breaches of Unsecured PHI in accordance with Paragraph E below and as required by 45 CFR § 164.410.

6. Contractor agrees to ensure that any Subcontractors that create, receive, maintain, or transmit PHI on behalf of Contractor agree to the same restrictions and conditions that apply through this Business Associate Contract to Contractor with respect to such information.

7. Contractor 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.

8. Contractor 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. Contractor agrees to notify County in writing no later than ten (10) calendar days after said amendment is completed.

9. Contractor agrees to make internal practices, books, and records, including policies and procedures, relating to the use and disclosure of PHI received from, or created or received by Contractor on behalf of, 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.

10. Contractor agrees to document any Disclosures of PHI County discloses to Contractor or Contractor 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.

11. Contractor 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 the Agreement, 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.

12. Contractor agrees that to the extent Contractor carries out County's obligation under the HIPAA Privacy and/or Security rules Contractor will comply with the requirements of 45 CFR Part 164 that apply to County in the performance of such obligation.

13. Contractor shall work with County upon notification by Contractor to County of a Breach to properly determine if any Breach exclusions exist as defined in Subparagraph B.2.a above.

D. SECURITY RULE

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

2. Contractor shall ensure that any subcontractors that create, receive, maintain, or transmit electronic PHI on behalf of Contractor agree through a contract with Contractor to the same restrictions and requirements contained in this Paragraph D of this Business Associate Contract.

3. Contractor shall report to County immediately any Security Incident of which it becomes aware. Contractor shall report Breaches of Unsecured PHI in accordance with Paragraph E below and as required by 45 CFR § 164.410.

E. BREACH DISCOVERY AND NOTIFICATION

1. Following the discovery of a Breach of Unsecured PHI , Contractor 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.

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

b. Contractor 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 Contractor, as determined by federal common law of agency.

2. Contractor shall provide the notification of the Breach immediately to the County Privacy Officer at

Andrew Alipanah, MBA, CISSP Chief Information Security Officer 721 S. Parker St. Suite 200 Orange, CA 92868 Phone: (714) 567-7611 Andrew.Alipanah@ocit.ocgov.com	Linda Le, CHPC, CHC, CHP County Privacy Officer 721 S. Parker St. Suite 200 Orange, CA 92868 Phone: (714) 834-4082 Linda.Le@ocit.ocgov.com

a. Contractor's notification may be oral, but shall be followed by written notification within 24 hours of the oral notification.

3. Contractor's notification shall include, to the extent possible:

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

b. Any other information that County is required to include in the notification to Individual under 45 CFR §164.404 (c) at the time Contractor 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:

(1) A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;

(2) 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);

(3) Any steps Individuals should take to protect themselves from potential harm resulting from the Breach;

(4) A brief description of what Contractor is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any future Breaches; and

(5) 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.

4. County may require Contractor 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.

5. In the event that Contractor is responsible for a Breach of Unsecured PHI in violation of the HIPAA Privacy Rule, Contractor shall have the burden of demonstrating that Contractor made all notifications to County consistent with this Paragraph E 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.

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

7. Contractor shall provide to County all specific and pertinent information about the Breach, including the information listed in Section E.3.b.(1)-(5) above, 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 Contractor's initial report of the Breach to County pursuant to Subparagraph E.2 above.

8. Contractor 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. Contractor 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.

9. Contractor shall bear all expense or other costs associated with the Breach and shall reimburse County for all expenses County incurs in addressing the Breach and consequences thereof, including costs of investigation, notification, remediation, documentation or other costs associated with addressing the Breach.

F. PERMITTED USES AND DISCLOSURES BY CONTRACTOR

1. Contractor may use or further disclose PHI County discloses to Contractor as necessary to perform functions, activities, or services for, or on behalf of, County as specified in the Agreement, 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.

a. Contractor may use PHI County discloses to Contractor, if necessary, for the proper management and administration of Contractor.

b. Contractor may disclose PHI County discloses to Contractor for the proper management and administration of Contractor or to carry out the legal responsibilities of Contractor, if:

i. The Disclosure is required by law; or

ii. Contractor 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 Contractor of any instance of which it is aware in which the confidentiality of the information has been breached.

c. Contractor may use or further disclose PHI County discloses to Contractor to provide Data Aggregation services relating to the Health Care Operations of Contractor.

2. Contractor may use PHI County discloses to Contractor, if necessary, to carry out legal responsibilities of Contractor.

3. Contractor may use and disclose PHI County discloses to Contractor consistent with the minimum necessary policies and procedures of County.

4. Contractor may use or disclose PHI County discloses to Contractor as required by law.

G. OBLIGATIONS OF COUNTY

1. County shall notify Contractor 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 Contractor's Use or Disclosure of PHI.

2. County shall notify Contractor of any changes in, or revocation of, the permission by an Individual to use or disclose his or her PHI, to the extent that such changes may affect Contractor's Use

or Disclosure of PHI.

3. County shall notify Contractor 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 Contractor's Use or Disclosure of PHI.

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

H. BUSINESS ASSOCIATE TERMINATION

1. Upon County's knowledge of a material breach or violation by Contractor of the requirements of this Business Associate Contract, County shall:

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

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

2. Upon termination of the Agreement, Contractor shall either destroy or return to County all PHI Contractor received from County or Contractor created, maintained, or received on behalf of County in conformity with the HIPAA Privacy Rule.

a. This provision shall apply to all PHI that is in the possession of Subcontractors or agents of Contractor.

b. Contractor shall retain no copies of the PHI.

c. In the event that Contractor determines that returning or destroying the PHI is not feasible, Contractor 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, Contractor 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 Contractor maintains such PHI.

3. The obligations of this Business Associate Contract shall survive the termination of the Agreement.