AGENDA STAFF REPORT

Control: 26001328

MEETING DATE:	06/23/2026
LEGAL ENTITY TAKING ACTION:	Board of Supervisors
BOARD OF SUPERVISORS DISTRICT(S):	District 5
SUBMITTING AGENCY/DEPARTMENT:	John Wayne Airport
DEPARTMENT CONTACT PERSON(S):	Charlene Reynolds, 949-252-5183 Richard Steele, 949-252-5264

SUBJECT: Approve Contract for Hardware and Software Maintenance Services

CEO CONCUR	COUNTY COUNSEL REVIEW	CLERK OF THE BOARD
Concur	Approve agreement to form	DISCUSSION 3 Votes Board Majority

Budgeted: N/A	**Current Year Cost:** N/A	**Annual Cost:** FY 2026-2027 $91,292 FY 2027-2028 $94,935 FY 2028-2029 $98,726 FY 2029-2030 $102,668 FY 2030-2031 $106,769
Staffing Impact: No		**Sole Source:** Yes
Current Fiscal Year Revenue: N/A	**Funding Source:** Fund 280: 100%	**County Audit in Last 3 years:** No
Levine Act Review Completed? Yes		
Prior Board Action: N/A		

RECOMMENDED ACTION(S):

1. Find that the proposed project is Categorically Exempt from the California Environmental Quality Act, Class 1 (Existing Facilities) pursuant to CEQA Guidelines Section 15301.
2. Authorize the County Procurement Officer or Deputized designee to execute a Sole Source Contract with Transcore, LP for Hardware and Software Maintenance Services, effective September 1, 2026, through August 31, 2031, in a total amount not to exceed $494,390.

SUMMARY:

Approval of a Sole Source Contract MA-280-26011292 with TransCore, LP provides hardware and software maintenance services for John Wayne Airport's Automated Vehicle Identification system, which is used to manage, track, monitor, and collect payment from ground transportation operators.

BACKGROUND INFORMATION:

TransCore, LP (Transcore) is a U.S.-based technology company that is the primary provider of electronic tolling and express lanes systems used by eight of the ten largest toll agencies in the United States, as well as several large and medium hub airports. The primary system components include: 1) the TransCore ground transportation Automated Vehicle Identification (AVI) hardware consisting of radio-frequency identification (RFID) transponders and readers, 2) the GateKeeper Commercial Vehicle Management System and Transportation Network Company trip and fee management software, and 3) the AdComp secure, online payment processing, invoicing, and permit management portal. These components are often used together as an integrated, turnkey solution for the management of airport ground transportation and commercial vehicle operators to include: shuttles, taxis, limousines, and Transportation Network Companies (TNC or Ride App services) that provide pick-up and drop-off services for John Wayne Airport (JWA) customers.

Non-TNC Operators: ground transportation vehicles carry an RFID transponder with a unique identification code or report trip activities through an application-based program. AVI readers and antennas mounted on the JWA roadways track and record the number of times each vehicle passes through JWA. A per-trip charge is applied to the vehicle operator, and transponders are provided at no cost to ground transportation services. Transcore provides vehicle transponders, transponder codes, antennae, and software for capturing trip data. The AVI system technology provided by Transcore is proprietary.

The Transcore system also identifies transponders used by other public agencies in the area, including Los Angeles International Airport. As a result, transponders can be identified and fees charged without an operator having to register independently with multiple agencies. The proposed Contract with Transcore includes hardware and software maintenance services, including emergency repairs and periodic software updates.

TNC Operators: these operators are not issued AVI transponders, but are tracked by the GateKeeper software, which sends data in near-real time from the TNC company. This enables JWA and other airports to validate fee payments, audit/analyze trip activity, and generate metric-based reports.

The proposed Contract MA-280-26011292 is a Sole Source procurement because the proprietary AVI system in use at JWA can only be serviced and supported by one vendor. Transcore is the exclusive authorized provider with trained and certified technicians required to service, maintain and support the existing AVI infrastructure. No other vendor is authorized or qualified to work on JWA's current system. The AVI system relies heavily on the specialized GateKeeper Commercial Vehicle Management Software application. Due to intellectual property restrictions, all software-related services, including updates, troubleshooting, and integration, must be performed solely by Transcore.

Replacing the existing AVI system would cost approximately $1.5 million, including hardware, software, transponder replacement, and transition coordination with JWA's commercial ground transportation providers and other transportation agencies.

JWA is procuring these services in accordance with Section 4.5 of the 2026 Contract Policy Manual. The Orange County Preference Policy is not applicable to Sole Source contracts.

The Board of Supervisors (Board) has previously approved multiple Sole Source contracts with Transcore for maintenance and support of JWA's AVI system. On November 22, 2011, the Board approved a Sole Source Contract with Transcore for the purchase of JWA's AVI hardware and software maintenance. The Board later approved a new three-year Sole Source Contract for the same services on August 22, 2017.

On March 26, 2020, the Board authorized a COVID-19 Resolution that allowed extensions to County of Orange contracts during the state of emergency. Under this authority, JWA executed a one-year Sole Source Contract with Transcore on August 28, 2020, which expired on August 31, 2021.

Subsequently, on July 27, 2021, the Board approved another Sole Source Contract with Transcore, effective September 1, 2021, through August 31, 2026, in a total amount not to exceed $443,128.

JWA recommends Board approval of the proposed five-year Sole Source Contract with Transcore for hardware and software maintenance services at a cost of $494,390, effective September 1, 2026, through August 31, 2031.

Contractor performance has been confirmed as satisfactory. JWA has conducted due diligence on Transcore and has verified that there are no concerns that must be addressed with respect to the contractor's ownership/name, litigation status, or conflicts with County interests. An analysis was completed to verify the contract provides County with persons specially trained, experienced, expert and competent to perform the special services in accordance with the law.

This Sole Source Contract includes two subcontractors that will provide operators with the ability to view and pay their trip charges online. See Attachment B for information regarding subcontractors and the Contract Summary Form.

At the end of the five-year term, JWA will reevaluate the performance, functionality, and cost effectiveness of the current system. This assessment will include a review of available alternatives and an analysis of whether transitioning the services to a competitive procurement is feasible and in JWA's best interest. The results of this evaluation will guide the Airport's determination of the appropriate next steps.

COMPLIANCE WITH CEQA: The proposed project is categorically exempt (Class 1) from the provisions of CEQA pursuant to CEQA Guidelines Section 15301, because it involves maintenance and repair of existing public facilities and mechanical equipment associated with John Wayne Airport's Automated Vehicle Identification system, involving negligible or no expansion of the existing use.

FINANCIAL IMPACT:

Appropriations for this Contract will be included in Airport Operating Fund 280 FY 2026-27 Budget, and will be included in the budgeting process for future years.

The proposed Contract includes provisions stating that the Contract is subject to and contingent upon applicable budgetary appropriations approved by the Board for each fiscal year during the term of the Contract. If such appropriations are not approved or are reduced, the Contract may be immediately modified or terminated without penalty to the County. The Contract contains language allowing JWA to terminate the Contract, reduce the scope of services, and/or renegotiate the scope of services to be provided.

STAFFING IMPACT:

N/A

REVIEWING AGENCIES/DEPARTMENTS:
N/A

ATTACHMENTS:
Attachment A - Contract MA-280-26011292 with Transcore LP
Attachment B - Contract Summary Form

CONTRACT MA-280-26011292

FOR

HARDWARE AND SOFTWARE MAINTENANCE SERVICES

BETWEEN

JOHN WAYNE AIRPORT

AND

TRANSCORE, LP

JOHN WAYNE AIRPORT
ORANGE COUNTY

CONTRACT MA-280-26011292
WITH
TRANSCORE, LP
FOR
HARDWARE AND SOFTWARE MAINTENANCE SERVICES

This Contract MA-280-26011292 Hardware and Software Maintenance Services ("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; (hereinafter referred to as "County") and TransCore, LP, with a place of business at 3410 Midcourt Rd Ste 102, Carrollton, TX 75006-4995 (hereinafter referred to as "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/Compensation
Attachment C – County of Orange Information Technology Security Guidance
Attachment D – Key Personnel/Staffing Plan
Attachment E – GSI - Cyber Security Enhancements
Attachment F – SNA - Software Maintenance Agreement with AdComp - 2026

RECITALS

WHEREAS, Contractor and County are entering into this Contract for Hardware and Software Maintenance Services under a firm fixed fee Contract; and

WHEREAS, Contractor agrees to provide Hardware and Software Maintenance Services 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

WHEREAS, the County Board of Supervisors has authorized the Deputy Procurement Agent or designee to enter into a Contract for Hardware and Software Maintenance Services with the Contractor;

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

DEFINITIONS

DPA shall mean the Deputy Procurement Agent assigned to this Contract.

ARTICLES

General Terms and Conditions:

A. **Governing Law and Venue:** This Contract has been negotiated and executed in the state of California and shall be governed by and construed under the laws of the state of California. 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.

B. **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.

C. **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.

D. **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 the Contractor.

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

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

G. **Warranty:** Contractor expressly warrants that the goods 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 paragraph "Z" below, and as more fully described in paragraph "Z," 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.

H. **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 paragraph "Z" below, it shall indemnify, defend, and hold County and County Indemnitees harmless from any and all such claims and be responsible for payment of all costs, damages, penalties and expenses related to or arising from such claim(s), including, costs and expenses but not including attorney's fees.

I. **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.

J. **Civil Rights and Nondiscrimination:**

1. **General Civil Rights Provisions:** In all its activities within the scope of its airport program, the Contractor agrees to comply with pertinent statutes, Executive Orders, and such rules as identified in Title VI List of Pertinent Nondiscrimination Acts and Authorities to ensure that no person shall, on the grounds of race, color, national origin, creed, sex, age, or disability be excluded from participating in any activity conducted with or benefiting from Federal assistance.

   This provision is in addition to that required by Title VI of the Civil Rights Act of 1964.

   The above provision binds the Contractor and subcontractors from the bid solicitation period through the completion of the contract.

2. **Nondiscrimination:** 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.

3. **Compliance with Nondiscrimination Requirements:** During the performance of this contract, the Contractor, for itself, its assignees, and successors in interest (hereinafter referred to as the "Contractor"), agrees as follows:

   a. **Compliance with Regulations:** The Contractor (hereinafter includes consultants) will comply with the Title VI List of Pertinent Nondiscrimination Acts and Authorities, as they may be amended from time to time, which are herein incorporated by reference and made a part of this contract.

   b. **Nondiscrimination:** The Contractor, with regard to the work performed by it during the contract, will not discriminate on the grounds of race, color, national origin, creed, sex, age, or disability in the selection and retention of subcontractors, including procurements of materials and leases of equipment. The Contractor will not participate directly or indirectly in the discrimination prohibited by the Nondiscrimination Acts and Authorities, including employment practices when the contract covers any activity, project, or program set forth in Appendix B of 49 CFR part 21 including amendments thereto.

   c. **Solicitations for Subcontracts, including Procurements of Materials and Equipment:** In all solicitations, either by competitive bidding or negotiation made by the Contractor for work to be performed under a subcontract, including procurements of materials, or leases of equipment, each potential subcontractor or supplier will be notified by the Contractor of the contractor's obligations under this Contract and the Nondiscrimination Acts and Authorities on the grounds of race, color, or national origin.

   d. **Information and Reports:** The Contractor will provide all information and reports required by the Acts, the Regulations, and directives issued pursuant thereto and will permit access to its books, records, accounts, other sources of information, and its facilities as may be determined by the Sponsor or the Federal Aviation Administration to be pertinent to ascertain compliance with such

Nondiscrimination Acts and Authorities and instructions. Where any information required of a contractor is in the exclusive possession of another who fails or refuses to furnish the information, the Contractor will so certify to the Sponsor or the Federal Aviation Administration, as appropriate, and will set forth what efforts it has made to obtain the information.

e. **Sanctions for Noncompliance:** In the event of a Contractor's noncompliance with the nondiscrimination provisions of this contract, the Sponsor will impose such contract sanctions as it or the Federal Aviation Administration may determine to be appropriate, including, but not limited to:

   i. Withholding payments to the Contractor under the contract until the Contractor complies; and/or

   ii. Cancelling, terminating, or suspending a contract, in whole or in part.

f. **Incorporation of Provisions:** The Contractor will include the provisions of paragraphs (a) through (f) in every subcontract, including procurements of materials and leases of equipment, unless exempt by the Acts, the Regulations, and directives issued pursuant thereto. The Contractor will take action with respect to any subcontract or procurement as the Sponsor or the Federal Aviation Administration may direct as a means of enforcing such provisions including sanctions for noncompliance. Provided, that if the Contractor becomes involved in, or is threatened with litigation by a subcontractor, or supplier because of such direction, the Contractor may request the Sponsor to enter into any litigation to protect the interests of the Sponsor. In addition, the Contractor may request the United States to enter into the litigation to protect the interests of the United States.

Upon request by the County, Contractor will provide a copy of each subcontract to demonstrate the above language has been inserted.

4. **Title VI List of Pertinent Nondiscrimination Acts and Authorities:** During the performance of this Contract, the Contractor, for itself, its assignees, and successors in interest (hereinafter referred to as the "Contractor") agrees to comply with the following nondiscrimination statutes and authorities; including but not limited to:

- Title VI of the Civil Rights Act of 1964 (42 USC § 2000d *et seq*., 78 stat. 252) (prohibits discrimination on the basis of race, color, national origin);
- 49 CFR part 21 (Nondiscrimination in Federally-Assisted programs of the Department of Transportation—Effectuation of Title VI of the Civil Rights Act of 1964) including amendments thereto;
- The Uniform Relocation Assistance and Real Property Acquisition Policies Act of 1970, (42 USC § 4601) (prohibits unfair treatment of persons displaced or whose property has been acquired because of Federal or Federal-aid programs and projects);
- Section 504 of the Rehabilitation Act of 1973 (29 USC § 794 *et seq*.), as amended (prohibits discrimination on the basis of disability); and 49 CFR part 27 (Nondiscrimination on the Basis of Disability in Programs or Activities Receiving Federal Financial Assistance);
- The Age Discrimination Act of 1975, as amended (42 USC § 6101 *et seq*.) (prohibits discrimination on the basis of age);
- Airport and Airway Improvement Act of 1982 (49 USC § 47123), as amended (prohibits discrimination based on race, creed, color, national origin, or sex);
- The Civil Rights Restoration Act of 1987 (PL 100-259) (broadened the scope, coverage and applicability of Title VI of the Civil Rights Act of 1964, the Age Discrimination Act of 1975 and Section 504 of the Rehabilitation Act of 1973, by expanding the definition of the terms "programs or activities" to include all of the programs or activities of the Federal-aid recipients, sub-recipients and contractors, whether such programs or activities are Federally funded or not);
- Titles II and III of the Americans with Disabilities Act of 1990 (42 USC § 12101, et seq), (prohibit

discrimination on the basis of disability in the operation of public entities, public and private transportation systems, places of public accommodation, and certain testing entities) as implemented by U.S. Department of Transportation regulations at 49 CFR parts 37 and 38;

- Title IX of the Education Amendments of 1972, as amended, which prohibits you from discriminating because of sex in education programs or activities (20 USC § 1681, et seq).

Contractor is required to insert the above Title VI List of Pertinent Nondiscrimination Acts and Authorities into every subcontract at any tier. Upon request by the County, Contractor will provide a copy of each subcontract to demonstrate that the above language has been inserted.

5. **Civil Rights Training:** Upon request by the County, Contractor is required to disseminate and provide training materials and other information related to Title VI Civil Rights to its staff as specified by the County.

K. **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 the Contractor. Exercise by County of its right to terminate the Contract shall relieve County of all further obligation.

L. **Consent to Breach Not Waiver:** No term or provision of this Contract shall be deemed waived, and no breach excused, unless such waiver or consent shall be in writing and signed by the party claimed to have waived or consented. Any consent by any party to, or waiver of, a breach by the other, whether express or implied, shall not constitute consent to, waiver of, or excuse for any other different or subsequent breach.

M. **Independent Contractor:** 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.

N. **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 goods/services furnished by the 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.

O. **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).**

If the insurance carrier does not have an A.M. Best Rating of A-/VIII, CEO/ 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:

Coverage	Minimum Limits
Commercial General Liability	$1,000,000 per occurrence $2,000,000 aggregate
Automobile Liability including coverage for owned or scheduled, non-owned, and hired vehicles	$1,000,000 combined single limit each accident
Workers Compensation	Statutory
Employers Liability Insurance	$1,000,000 per accident or disease
Network Security & Privacy Liability	$1,000,000 per claims-made
Technology Errors & Omissions	$1,000,000 per claims-made $1,000,000 aggregate

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

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.

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

Required Endorsements

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

1) 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.

2) 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.

3) 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, employees, and agents*** or provide blanket coverage, which will state ***As Required by Written Contract***.

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

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

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

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.

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).

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.

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

Q. **Change of Ownership, 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 the County agrees to an assignment of the Contract, the new owners shall be required under terms of sale or other transfer to assume Contractor's duties and obligations contained in this Contract and complete them to the satisfaction of the County.

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

In addition, Contractor has the duty to notify the County in writing of any change in the Contractor's status with respect to name changes that do not require an assignment of the Contract. The Contractor is also obligated to notify the County in writing if the Contractor becomes a party to any litigation against the County, or a party to litigation that may reasonably affect the Contractor's performance under the 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 the County any time there is a change in Contractor's name, conflict of interest or litigation status, Contractor must also provide an update to the County of its status in these areas whenever requested by the County.

The 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 the Contractor, this obligation shall apply to the Contractor's employees, agents, and subcontractors associated with the provision of goods and services provided under this Contract. The 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.

R. **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.

S. **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.

T. **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 paragraph "Z" below, 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.

U. **Freight:** Prior to the 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 this Contract.

V. **Severability:** If any term, covenant, condition or provision of this Contract is held by a court of competent jurisdiction to be invalid, void, or 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.

W. **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.

X. **Interpretation:** This Contract has been negotiated at arm's length and between persons sophisticated and knowledgeable in the matters dealt with in this Contract. In addition, each party 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.

Y. **Employee Eligibility Verification:** The 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. The 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. The Contractor shall retain all such documentation for all covered employees for the period prescribed by the law. The Contractor shall indemnify, defend with counsel approved in writing by County, and hold harmless, the County, its agents, officers, and employees from employer sanctions and any other liability which may be assessed against the Contractor or the County or both in connection with any alleged violation of any Federal or State statutes or regulations pertaining to the eligibility for employment of any persons performing work under this Contract.

Z. **Indemnification:** 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.

AA. **Audits/Inspections:** Contractor agrees to permit the County's Auditor-Controller or the Auditor-Controller's authorized representative (including auditors from a private auditing firm hired by the County) access during normal working hours to all books, accounts, records, reports, files, financial records, supporting documentation, including payroll and accounts payable/receivable records, and other papers or property of 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 the Contract including, but not limited to, the costs of administering the Contract. The County will provide reasonable notice of such an audit or inspection.

The County reserves the right to audit and verify the 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 the County to audit records and interview staff of any subcontractor related to performance of this Contract.

Should the Contractor cease to exist as a legal entity, the Contractor's records pertaining to this Contract shall be forwarded to the County's Project Manager.

BB. **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.

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

DD. **California Public Records Act:** Contractor and County agree and acknowledge that all information and documents related to the award and performance of this Contract may be subject to disclosure pursuant to the California Records Act, California Government Code Section 79200.000 et seq. Contractor shall not respond to any California Public Records Act request directed at County; all responses shall be handled by County.

Additional Terms and Conditions:

1. **Scope of Contract:** This Contract specifies the contractual terms and conditions by which the County will procure Hardware and Software Maintenance Services from Contractor as further detailed in the Scope of Work, identified, and incorporated herein by this reference as "Attachment A".

2. **Term of Contract:** The initial term of this Contract shall become effective September 1, 2026, and shall continue for five (5) years, unless otherwise terminated as provided herein.

3. **Amendments – Changes/Extra Work:** The Contractor shall make no changes to this Contract without the County's written consent. In the event that there are new or unforeseen requirements, the County with the Contractor's concurrence has the discretion to request official changes at any time without changing the intent of this Contract.

   If County-initiated changes or changes in laws or government regulations affect price, the Contractor's ability to deliver services, or the project schedule, the Contractor shall give the County written notice no later than

seven calendar days from the date the law or regulation went into effect or the date the change was proposed by the County and the Contractor was notified of the change. Such changes shall be agreed to in writing and incorporated into a Contract amendment. Said amendment shall be issued by the County assigned Deputy Procurement Agent, shall require the mutual consent of all parties, and may be subject to approval by the County Board of Supervisors. Nothing herein shall prohibit the Contractor from proceeding with the work as set forth in this Contract.

4. **Adjustments – Scope of Work:** No adjustments made to the Scope of Work will be authorized without prior written approval of the County assigned Deputy Procurement Agent.

5. **Americans with Disabilities Act (ADA):** Contractor shall comply with Section 504 of the Rehabilitation Act of 1973 as amended; Title VI and VII of the Civil Rights Act of 1964 as amended; Americans with Disabilities Act, 42 USC 12101 et seq; California Code of Regulations, Title 2, Title 22: California Government Code, Sections 11135, et seq; and other federal and state laws and executive orders prohibit discrimination. All programs, activities, employment opportunities, and services must be made available to all persons, including persons with disabilities.

6. **Breach of Contract:** The failure of the 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 the County may, and in addition to any other remedies available at law, in equity, or otherwise specified in this Contract:

   a) Terminate the Contract immediately, pursuant to Section K herein;

   b) Afford the 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 the Contractor is in breach; and

   d) Offset against any monies billed by the Contractor but yet unpaid by the County those monies disallowed pursuant to the above.

7. **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.

a. 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, County of Orange Information Technology Security Guidelines and Business Associate Contract, as applicable.

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.

b. 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.

c. 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.

d. 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.

e. 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.

f. 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.

    i. 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.

ii. 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.

g. 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.

h. 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

i. 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.

j. 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.

8. **Computer Hardware and Software Standards:** No substitution of hardware or software will be accepted. The specifications provided herein are approved County of Orange standards.

9. **Conditions Affecting Work:** The 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 the Contractor to do so will not relieve Contractor from responsibility for successfully performing the work without additional cost to the County. The County assumes no responsibility for any understanding or representations concerning the nature, location(s) or general conditions made by any of its officers or agents prior to the execution of this Contract, unless such understanding or representations by the County are expressly stated in the Contract.

10. **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.

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

    The Contractor's Project Manager shall be assigned to this project for the duration of the Contract and shall diligently pursue all work and services to meet the project timelines. The County's Project Manager shall have the right to require the removal and replacement of the Contractor's Project Manager from providing services to the County under this Contract. The County's Project manager shall notify the Contractor in writing of such action. The Contractor shall accomplish the removal within five (5) business days after written notice by 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. 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.

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

13. **Default – Reprocurement Costs:** In case of Contract breach by Contractor, resulting in termination by the County, the County may procure the goods and/or services from other sources. If the cost for those goods and/or services is higher than under the terms of the existing Contract, Contractor will be responsible for paying the County the difference between the Contract cost and the price paid, and the County may deduct this cost from any unpaid balance due the Contractor. The price paid by the 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.

14. **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, such matter shall be brought to the attention of the County Deputy Procurement Agent by way of the following process:

    A. The Contractor shall submit to the agency/department assigned Deputy Procurement 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 the 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 the Contract, the 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 the Contract adjustment for which the Contractor believes the County is liable.

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

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

15. **Drug-Free Workplace:** The Contractor hereby certifies compliance with Government Code Section 8355 in matters relating to providing a drug-free workplace. The 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.

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

1) The Contractor has made false certification, or

2) The Contractor violates the certification by failing to carry out the requirements as noted above.

16. **EDD Independent Contractor Reporting Requirements:** Effective January 1, 2001, the 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 the County pays $600 or more or with whom the 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 web site located at http://www.edd.ca.gov/Employer_Services.htm.

17. **Errors 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.

18. **Equal Employment Opportunity:** The 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. The 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, the 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. The 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. The 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.

19. **Equipment – Acceptance Testing:** Acceptance testing is intended to ensure that the equipment acquired operates in substantial accord with the Contractor's technical specifications, is adequate to perform as warranted by the Contractor, and evidences a satisfactory level of performance reliability prior to its acceptance by the County. If the equipment to be installed includes operating software as listed in the Contract or order, such operating software shall be present for the acceptance test unless substitute operating software acceptable to the County is provided. Acceptance testing may be required as specified in the Contract or order for all newly installed technology systems, subsystems, and individual equipment, and machines which are added or field modified, i.e. modification of a machine from one model to another, after a successful performance period.

20. **Equipment – Maintenance:** If the Contractor is unable to perform maintenance or the County desires to perform its own maintenance on equipment purchased under this contract, then, upon written notice by the County, the Contractor will provide, at Contractor's then current rates and fees, adequate and reasonable assistance, including relevant documentation, to allow the County to maintain the equipment based on the Contractor's methodology. The Contractor agrees that the County may reproduce such documentation for its own use in maintaining the equipment. If the Contractor is unable to perform maintenance, the Contractor agrees to license any other Contractor that the County may have hired to maintain the equipment to use the above-noted documentation.

    The County agrees to include the Contractor's copyright notice on any such documentation reproduced, in accordance with copyright instruction to be provided by the Contractor.

21. **Equipment – Title to:** Unless otherwise specified in the Contract, order, or finance plan, title to the equipment shall remain with the Contractor and assigns, if any, until such time as the full purchase prices, applicable taxes, and interest charges, if any, are paid to the Contractor. Title to each machine will be transferred to the County when its purchase price, taxes, and associated interest charges, if any, are paid. Title to a special feature installed on a machine and for which only a single installation charge was paid shall pass to the County at no additional charge, together with title to the machine on which it was installed.

22. **Freight Changes:** If shipping charges are included in the Contract, the Contractor must prepay those shipping charges and include them in the invoice to the County. All invoices with prepaid shipping charges over $50.00 must be accompanied by a copy of the freight bill.

23. **Gratuities:** The Contractor warrants that no gratuities, in the form of entertainment, gifts or otherwise, were offered or given by the Contractor or any agent or representative of the Contractor to any officer or employee of the County with a view toward securing the Contract or securing favorable treatment with respect to any determinations concerning the performance of the Contract. For breach or violation of this warranty, the

County shall have the right to terminate the Contract, either in whole or in part, and any loss or damage sustained by the County in procuring on the open market any goods or services which the Contractor agreed to supply shall be borne and paid for by the Contractor. The rights and remedies of the County provided in the clause shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Contract.

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

25. **News/Information Release:** The 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 the County through the 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 Deputy Procurement Agent (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:	Transcore, LP Attn: Forrest Swonsen 3410 Midcourt Rd, Ste. 102 Carrollton, TX 75006 Phone: (972) 342-1431 Email: forrest.swonsen@transcore.com
County's Project Manager:	Attn: Robert Holden 18601 Airport Way, #41 Santa Ana, CA 92707 Phone: (949) 252-5246 Email: rholden@ocair.com
cc:	JWA/Procurement Services Attn: Choy Pham, County DPA 3160 Airway Avenue Costa Mesa, CA 92626 Phone: (949) 252-5128 Email: cpham@ocair.com

27. **OEM Equipment Maintenance Standard:** The Contractor agrees to maintain all equipment according to the original equipment manufacturer (OEM) specifications. The Contractor further agrees that all components will be OEM components. At the termination of the Contract the Contractor guarantees that equipment will meet OEM equipment certification standards.

28. **Precedence:** The Contract documents consist of this Contract and its exhibits and attachments. In the event of a conflict between or among the 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.

29. **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.

30. **Provision of Services:** County may call upon Contractor to immediately provide Services during or in anticipation or remediation of emergencies of any kind whatsoever as determined solely by County. To the maximum extent practicable and lawful under such circumstances, Contractor shall prioritize the deployment of labor, equipment, and/or supplies pursuant to this Contract above all other interests and obligations. Upon contact for assistance with and emergency, Contractor shall indicate within 10 minutes whether the requested labor, equipment, and supplies are available. County shall then direct Contractor to mobilize resources based on information provided by County's Representative. County's Representative shall function as incident command unless otherwise notified and shall direct all on-scene operations by Contractor. Notwithstanding any other provision of this Contract, County's direction of Contractor's Provision of Services need not be in writing, but may be in-person or via telephone, radio, text message, email or other means.

31. **Software – Acceptance:** The County shall be deemed to have accepted each software product unless the County, within 30 days from the installation date, gives Contractor written notice to the effect that the software product fails to conform to the functional and performance specifications, which, if not attached, are incorporated by reference. The Contractor will, upon receipt of such notice, investigate the reported deficiencies. The right of the parties shall be governed by the following:

    A. If it is found that the software product fails to conform to the specifications and the Contractor is unable to remedy the deficiency with 60 days, the County shall return all material furnished hereunder and this Contract shall be terminated.

    B. If it is found that the software product fails to conform to the specifications and the Contractor, within 60 days of receipt of the above said notice, corrects the deficiencies in the software product, the County will provide the Contractor with written acknowledgement of its acceptance of said software product.

    C. If it is found that the software product does, in fact, conform to the specifications, the County shall reimburse the Contractor for the time and material cost of the investigation at the rates specified in this Contract.

    The County's acceptance of the software product is contingent upon the software product conforming to function and performance specifications and the Contractor delivering adequate users manuals within 30 days from the installation date.

32. **Software – Acceptance Testing:** Acceptance testing may be required as specified for all Contractor-supplied software as specified and listed in the Contract or order, including all software initially installed. Included in this clause are improved versions, including new releases, of this software, any such software which has been modified by the Contractor to satisfy the County requirements, and any substitute software provided by the

Contractor in lieu thereof, unless the Contract or order provides otherwise. The purpose of the acceptance test is to ensure that the software operates in substantial accord with the Contractor's technical specifications and meets the County's performance specifications.

33. **Software – Future Releases:** If improvement, upgraded, or enhancement versions of any software product under this Contract are developed by the Contractor and are made available to other licensees, they will be made available to the County at the County's option, provided such versions are operable on the same computer hardware configuration. The charge for such upgrading to the later version of the software will be the difference between the price established by the Contractor for the later version and the price specified herein or the then prevailing prices of the currently installed version.

34. **Software – Installation:** The installation date for the software products shall be established in accordance with the provisions below:

    If the County elects to install the software products, the County will have 30 days from the date of receipt of the software products to initially install and evaluate the software. The date of expiration of this period shall hereafter be known as the "installation date." The Contractor shall be responsible for providing criteria and test data necessary to check out the software products.

    If installation by the Contractor is required by the County, the Contractor will have up to 30 days from the effective date of this Contract to provide initial installation and evaluation of the software products on the County's designated CPU. The Contractor will issue written notice of the fact that the software products are operational, and the date of said notice shall be known as the "installation date." It will be at the Contractor's discretion to determine the criteria and tests necessary to allow the Contractor to issue a notice to the effect that the system is operational.

    The County agrees to provide such access to its computer system as may be required by the Contractor to properly install and test the software products. The County further agrees to provide, at no cost to the Contractor, systems and production support as may be required by the Contractor during installation.

    If installation by the Contractor is required by the County, the Contractor will provide such installation on the County's equipment at the rates specified in this Contract.

35. **Software – Inventions, Discoveries, Improvements:** All inventions or discoveries of or improvements to computer programs developed pursuant to this Contract shall be the property of the County. The County agrees to grant a nonexclusive royalty-free license for any such invention, discovery or improvement to the Contractor or to any other such person and further agrees that the contactor or any other such person may sublicense additional persons on the same royalty-free basis.

    This Contract shall not preclude the Contractor from developing materials outside this Contract which are competitive, irrespective of their similarity to materials which might be delivered to the County pursuant to this Contract.

36. **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. Suspected errors discovered by the County in the software products will be handled by the following procedure:

    A. A listing of the output and a copy of the evidential input data in machine-readable format will be submitted to the Contractor along with a completed copy of the appropriate Contractor information form and, if appropriate, a listing of the contents of the memory of the CPU at the time the error was noted.

B. Errors in the software product as verified by the Contractor will be corrected by providing a new copy of said software product or a new copy of the affected portions in machine-readable format.

C. 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.

37. **Software – Protection:** The County agrees that all material appropriately marked or identified as proprietary, whether oral or written, and furnished hereunder are provided for County's exclusive use for the purposes of this agreement only and will be held in confidence. All proprietary data shall remain the property of the Contractor. County agrees to take all reasonable steps to ensure that such data are not disclosed to others without prior written consent of the Contractor. The County will ensure, prior to disposing of any media, that any licensed materials contained thereon have been erased or otherwise destroyed.

    The County agrees that it will take appropriate action by instruction, agreement or otherwise with its employees or other persons permitted access to licensed programs and/or optional materials to satisfy its obligations under this agreement with respect to use, copying, modification and protection and security of licensed programs and optional materials.

38. **Software – Right to Copy or Modify:** Any software product provided by the contractor in machine-readable format may be copied, in whole or in part, in printed or machine-readable format for use by the County with the designated CPU to perform one-time benchmark tests, for archival or emergency restart purposes, to replace a worn copy, to understand the contents of such machine-readable material, or to modify the software product as provided below, provided, however that no more than the County- and contractor-agreed to number of copies will be in existence under this contract at any one time without the prior written consent from the contractor. Such consent shall not be unreasonably withheld by the contractor. The original and any copies of the software product, in whole or in part, which are made hereunder shall be the property of the contractor.

    The County agrees to keep any such copies and the original at a contractor and County mutually designated County location, except that the County may transport or transmit a copy of the original of any software product to another County location for backup use when required by CPU malfunction, provided the copy or the original is destroyed or returned to the designated location when the malfunction is corrected.

    The County may modify any non-personal computer software product in machine–readable format for its own use and merge it into other program material. Any portion of the software product included in any merged program material shall be used only on the designated CPUs and shall be subject to the terms and conditions of this contract.

39. **Software – Subject to Fiscal Appropriations:** This Contract is subject to and contingent upon applicable budgetary appropriations being approved by the County of Orange Board of Supervisors for each fiscal year during the term of this Contract. If such appropriations are not approved, the Contract will be terminated without penalty to the County.

    County agrees that if the provisions of the paragraph above are invoked, all equipment and software furnished by the Contractor under the terms of this Contract which are not the property of the County shall be returned to the Contractor in substantially the same condition in which it was delivered to the County, subject to normal wear and tear. County further agrees to pay for packing, crating, transportation to the Contractor's nearest facility, and reimbursement to the Contractor for expenses incurred for their assistance in such packing and crating.

40. **Software Documentation:** The Contractor agrees to provide to the County the County-designated number of all manuals and other associated printed materials and updated versions thereof, which are necessary or useful to the County in its use of the equipment or software provided hereunder. The County will designate the number of copies for production use and the number of copies for disaster recovery purposes and will provide this information to the Contractor.
    If additional copies of such documentation are required, the Contractor will provide such manuals at the request of the County. The requesting agency/department shall be billed for the manuals and any associated costs thereto by invoice. The Contractor agrees to provide such additional manuals at prices not in excess of charges made by the Contractor to its best customers for similar publications.

    The Contractor further agrees that the County may reproduce such manuals for its own use in maintaining the equipment or software provided hereunder. The County agrees to include the Contractor's copyright notice on any such documentation reproduced in accordance with copyright instructions to be provided by the Contractor.

41. **Software License:** The Contractor hereby grants to the County of Orange and the County accepts from the Contractor, subject to the terms and conditions of this agreement, a non-exclusive, non-transferable license to use the software products list in this agreement, hereinafter referred to as "software products." The license granted above authorizes the County to use the software products in machine-readable form on a single computer system, designed in writing by the County to the Contractor, provided that if the designated CPU is inoperative due to malfunction, license herein granted shall be temporarily extended to authorize the County to use the software products in machine-readable form on any other County CPU until the designated CPU is returned to operation. By prior written notice to the Contractor the County may redesignate the CPU in which the software products are to be used and must do so if the redesignation is permanent.

    When encryption/CPU ID authorization codes are required to operate the software products, the Contractor will provide all codes to the County with shipment of the software. In the case of an inoperative CPU, as defined above, Contractor will provide a temporary encryption/CPU ID authorization code to the County for use on a temporarily authorized CPU until the designated CPU is returned to operation. When changes in designated CPUs occur, the Contractor will issue to the County within 24 hours of notification a temporary encryption/ID authorization code for use on the newly designated CPU until such time a permanent code is assigned.

42. **Software License – Fees and Charges:** Upon completion of installation and acceptance of software products by the County, the County will pay the license fee or recurring charge for the software products as set forth in this Contract. Charges will commence on the installation date as specified in this Contract. The Contractor shall render invoices for recurring charges or a single charge for the month for which the charges were incurred. Fees for a partial month's use will be prorated based on a thirty-day month. Invoices are to be submitted in arrears to the user agency/department to the ship-to address, unless otherwise directed in this Contract. Payment will be net 30 days after receipt of an invoice in a format acceptable to the 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 the Contractor.

43. **Solicitation Notice - Title VI Solicitation Notice:** The County, in accordance with the provisions of Title VI of the Civil Rights Act of 1964 (78 Stat. 252, 42 U.S.C. §§ 2000d to 2000d-4), 28 CFR § 50.3, and 49 CFR Part 21, hereby notifies all bidders that it will affirmatively ensure that any contract entered into pursuant to this advertisement, all contractors will be afforded full opportunity to submit bids in response to this invitation and will not be discriminated against on the grounds of the owner's race, color, national origin, sex, creed, age, or disability in consideration for an award.

44. **State Funds – Audits:** When and if state funds are used in whole or part to pay for the goods and/or services under this Contract, the Contractor agrees to allow the Contractor's financial records to be audited by auditors

from the State of California, the County of Orange, or a private auditing firm hired by the State or the County. The State or County shall provide reasonable notice of such audit.

45. **Stop Work:** The County may, at any time, by written stop work order to the Contractor, require the Contractor to stop all or any part of the work called for by this Contract for a period of 90 days after the stop work order is delivered to the Contractor and for any further period to which the parties may agree. The stop work order shall be specifically identified as such and shall indicate it is issued under this clause. Upon receipt of the stop work order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the stop work order during the period of work stoppage. Within a period of 90 days after a stop work order is delivered to the Contractor or within any extension of that period to which the parties shall have agreed, the County shall either:

    Cancel the stop work order; or Terminate work covered by the stop work order as provided for in the "Default" or "Termination" clause of this Contract.

    If a stop work order issued under this clause is canceled or the period of the stop work order or any extension thereof expires, the Contractor shall resume work. The County shall make an equitable adjustment in the delivery schedule, the Contract price, or both, and the Contract shall be modified in writing accordingly if:

    The stop work order results in an increase in the time required or in the Contractor's cost properly allocable to the performance of any part of this Contract; and

    The Contractor asserts its right to an equitable adjustment within 30 days after the end of the period of work stoppage, provided that if the County decides the facts justify the action, the County may receive and act upon a proposal submitted at any time before final payment under this Contract.

    If a stop work order is not canceled and the work covered by the stop work order is terminated in accordance with the provision entitled, "Termination" the County shall allow reasonable costs resulting from the stop work order in arriving at the termination settlement.

    If a stop work order is not canceled and the work covered by the stop work order is terminated for default, the County shall allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop work order.

    An appropriate equitable adjustment may be made in any related Contract of the Contractor that provides for adjustment and is affected by any stop work order under this clause. The County shall not be liable to the Contractor for loss of profits because of a stop work order issued under this clause.

    If any provisions of this agreement are invalid under any applicable statute or rule of law, they are, to that extent, omitted, but the remainder of this agreement shall continue to be binding upon the parties hereto.

46. **Subcontracting:** No performance of this Contract or any portion thereof may be subcontracted or otherwise delegated by the Contractor, in whole or in part, without first obtaining the prior express written consent of County. Any attempt by the Contractor to subcontract or delegate any performance of this Contract without the prior express written consent of the 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 the Contractor is authorized by the 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 for 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.

47. **Substitution:** The Contractor is required to meet all specifications and requirements contained herein. No substitutions will be accepted without prior County written approval.

48. **Termination – Orderly:** After receipt of a termination notice from the County of Orange, the Contractor may submit to the 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 the County upon written request of the Contractor. Upon termination County agrees to pay the Contractor for all services performed prior to termination which meet the requirements of the Contract, provided, however, that such compensation combined with previously paid compensation shall not exceed the total compensation set forth in the 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 the Contract.

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

50. **Waivers – Contract:** The failure of the County in any one or more instances to insist upon strict performance of any of the terms of this Contract or to exercise any option contained herein shall not be construed as a waiver or relinquishment to any extent of the right to assert or rely upon any such terms or option on any future occasion.

(*Signature Page Follows*)

Signature Page

IN WITNESS WHEREOF, the Parties hereto have executed this Contract on the date first above written.

TRANSCORE, LP*

If the Contractor is a corporation, signatures of two specific corporate officers are required as further set forth.

- The first corporate officer signature must be one of the following: 1) Chairman of the Board, 2) President, 3) Vice President; and
- The second corporate officer signature must be one of the following: 1) Secretary, 2) Assistant Secretary, 3) Chief Financial Officer, 4) Assistant Treasurer.

In the alternative, a single corporate signature is acceptable when accompanied by a corporate resolution demonstrating the legal authority of the signature to bind the company.

Signature	Name	Title	Date
Signed by: Michael Mauritz C15EDE15472B451...	Michael Mauritz	SVP, Business Segment Manager	/7/2026
Signature	Name	Title	Date

COUNTY OF ORANGE, a political subdivision of the State of California
COUNTY AUTHORIZED SIGNATURE:

Signature	Name	Title	Date
	Choy Pham	Deputy Procurement Agent	

APPROVED AS TO FORM:
County Counsel

Signature	Name	Title	Date
DocuSigned by: Mark Sanchez 5EE66EC8DA7B48F...	Mark Sanchez	**Deputy**	/11/2026

ATTACHMENT A
SCOPE OF WORK

I. Overview

Contractor shall provide all parts, labor, and materials for on and off-site hardware and software maintenance services for John Wayne Airport (JWA) Automated Vehicle Identification (AVI) System. The basic objective of the TransCore AVI System is to provide JWA and its patrons with an efficient, convenient, and rapid means for payment for usage at JWA. The AVI System demonstrates accurate and reliable billing capabilities for patrons, protects against fraudulent usage, and provides statistical data for auditing and planning purposes.

II. System Overview

The core of the AVI System consists of four fundamental components: reader, built-in radio frequency (RF) module, antenna, and the TransCore Toll Tag®. The system uses modulated back scatter techniques to identify tags mounted on objects which are within the read range of the antenna and which have been assigned a unique identification code (UID) specific for JWA and the vehicle. In the case of AVI applications, the Toll Tag is installed on commercial vehicles requiring frequent access to the JWA landside facilities. The RF module in the AVI System generates continuous-wave RF signal, which is broadcast by the antenna. When the tagged vehicle enters the reading zone of the antenna, the tag detects this signal, modifies it to include its UDC, and reflects this modified signal back to the antenna. The antenna receives the modified signal and transfers it to the RF module in the reader, which demodulates and pre-amplifies the signal. The reader processes the received information, including storing the UID and the time and day in which the transaction occurred and passes this data to an interfacing computer for further processing.

1. Computer Hardware

The AVI System consists of a central computer and several client computers all connected together via a local area network. The County will be responsible for the hardware maintenance of the AVI central computer, client machines, and the network connecting the clients to the AVI central computer while Contractor will be responsible for maintaining the CVM software.

a. The AVI central computer is a server class machine that was purchased by and is maintained by County. The Commercial Vehicle Management (CVM) software is installed on this server and is maintained by TransCore/GateKeeper. All transponder read data is transferred from the AVI readers to the AVI central computer.

b. The client PCs those workstations that access the CVM programs and data from the AVT central computer. Client PCs are maintained by County.

2. Radio Frequency Identification Hardware.

TransCore system radio frequency readers and antennas are provided for each lane to detect the presence of tags on vehicles approaching lanes. In addition to the readers and antennas, Contractor shall ensure that the equipment specified in this section is properly maintained and operational.

a. TransCore Reader: TransCore Encompass® 5 Multiprotocol Reader is an integrated non-toll, multi-protocol 915 MHz radio frequency identification (RFID) reader system that includes an RF transceiver board and processor in a single assembly.

b. TransCore Antenna: TransCore Universal Toll Antenna (UTA) broadcasts and receives radio frequency (RF) signals in the 902 to 928 MHz frequency band.

c. Tags: Tags used by County are the TransCore AT5540 Tags, the ATS510 Tags and eGo Plus Sticker Tags. Support for ISO 18000-6C Tags is also included.

i. The AT5540 is small (credit card-sized), lightweight and housed in a polycarbonate case and designed for inside windshield mount. The ATSS10 is larger, housed in a polycarbonate case, weatherproof, and is designed for vehicle roof mount.

ii. Each tag is encoded with a unique code identification number and will not wear out or lose its identity for any reason during normal use within the tags' advertised operational life. Factory programming of tags by Contractor includes special security characters to further prevent tag counterfeiting.

iii. The AT5540 Tags are discontinued and are replaced by the AT5944 Tag. The AT5944 Toll Tag is a full frame, battery-powered RF tag designed for interior mounting on a non-metallized windshield.

iv. eGo Plus Sticker Tag is a 915 MHz radio frequency programmable, beam-powered, windshield-mounted tag. Packaged as a flexible sticker, this tag is ideal for applications that require low-cost, easily installed tags. This tag supports Super eGo (SeGo), and ATA protocols.

v. ISO 18000-6C Tag is a 915 MHz radio frequency programmable, beam-powered, windshield-mounted tag currently used at LAX. TransCore's Encompass 5 reader can be upgraded under a separate contract to support this tag protocol along with currently issued County tag. This scope of work assumes the already priced upgrade to have been performed and maintenance support is included.

vi. All TransCore tags are available for purchase by County under a separate Purchase Order.

d. TransCore Handheld Reader: TransCore Encompass® 1d Handheld Reader combines TransCore RFID end cap reader and DAP's CES240 color mobile computer.

e. Additional Reader/Antenna Equipment:

i. DC power supply

ii. Check tags

iii. Digital I/0 board

iv. Amber/red lights

v. 20-amp breakers

vi. Uninterruptible Power Supply

f. Reader Count

Location	Lanes	Cabinets	Readers
Airport Entry - Upper Roadway	5	1	3
Airport Entry - Lower Roadway	5	1	3
Spare	0	0	1

3. **Computer Software**

The software for the AVI System is GateKeeper-developed application software and consists of the following covered software:

a. GateKeeper Commercial Vehicle Management (CVM) software

b. TNC-Ops™ Module

c. Financial Module (Adcomp software)

d. Software Monitoring

e. GateKeeper Vendor Website

Under this agreement, Contractor through GateKeeper Systems, Inc. (GSI) shall maintain in good working order the computer software licensed to the County and known as the GateKeeper Systems Commercial Vehicle Management (CVM) software, and other related software components supplied by GateKeeper Systems as listed above under covered software.

III. Hardware/Software Maintenance

1. **Computer Software**
   a. Software Support Services: Contractor shall provide software support, through GSI, to County as necessary to eliminate or correct software malfunctions and return software to normal operation. The categories of software support to be provided under this Contract include:
      i. Response to System Problems: GSI shall provide on-line telephone support to County personnel as needed each month for the period of the contract to remotely diagnose and make required changes to the CVM software as well as other system components. Support shall be provided by qualified GSI personnel familiar with the CVM system and software version installed at JWA.

      ii. System Monitoring: GSI shall configure a server monitoring and alert tool for software monitoring. For this software to be effective, the County will provide SMTP access for these alerts to reach email accounts within the gksys.com domain. Additionally, after Version 7, GSI alarm monitoring requires a secure webservice connection that must be open for complete monitoring service.

      iii. System Updates: The County will install "Critical Updates" for the Microsoft operating and SQL database systems as specified by the County internal process requirements. The County is responsible for installation of service packs on the production servers. GSI will work with the Airport and provide any appropriate recommendations for scheduling and installation in the production environment.

      iv. System Upgrade: This Software Maintenance Agreement includes a fully paid license for any new version of the software (listed above in the Covered Software section). The Airport is not required to implement all new versions of the software, GSI will support previous versions for 24 months after release of the newest version. Optional:

         - Upgrade included: This agreement includes the discounted cost of one software upgrade each year during the term of the agreement including enhancements and implementation costs such as planning, database conversion, installation, and on-line training if required. New versions of the CVS Software may require OS or SQL software upgrades as minimum database and server requirements change over time. GSI effort to support server operating system and/or database upgrades may incur additional cost

      v. Monitor reads from all lanes, to verify communication between the host system and antenna plazas.

      vi. Make sure the system is running error free.

   b. Period of Coverage: Telephone support is available 24 hours per day, 7 days per week.

   c. Support Request Procedure: County will identify in writing at the initiation of the Contract, personnel authorized to request assistance. When assistance is required, the responsible individual should call GateKeeper Systems as follows:

      - **GateKeeper Emergency Support: (866) 688-3404**

This number should be used for support issues that need immediate resolution. This number is answered 24 hours per day, 365 days per year. If the support specialist answering the phone cannot address the problem, the operator will record information about the request or problem and immediately contact the best available GSI specialist to respond.

- **GateKeeper Non-Emergency Support: (651) 365-0700**

This number should be used during normal business hours for issues or questions that do not need immediate resolution to maintain system operation.

E-mail messages may be sent to Support@gksys.com for non-emergency requests for support and information. It is understood these non-emergency requests are not monitored on weekends, holidays or after normal business hours.

d. Response Time: Priority support response times are provided under this contract. GSI shall respond immediately during normal business working hours (8:00am to 5:00pm, Monday through Friday local Minneapolis time) at all other times (nights, weekends, holidays, etc.), a response shall be made within 1.5 hours by a qualified software specialist.

e. Access: Software Maintenance is conditioned upon provision by the County to GSI of reasonable appropriate access to the system(s) running the Covered Software, including, but not limited to, passwords, system data, file transfer capabilities, and remote log-in-capabilities. GSI shall maintain security of the system and use such access only for the purposes of this Agreement and will comply with County standard security procedures.

f. Owner Responsibilities: County personnel making a request for assistance should be prepared to provide detailed information regarding the problem experienced, actions already taken to remedy the problem and current operating condition of the software and entire system.

2. **AVI Hardware Support**

a. Contractor shall respond to AVI equipment service calls no later than the following business day.

b. Contractor shall perform Preventive Maintenance (PM) on the AVI hardware located in the lanes and roadside enclosure cabinet quarterly. The reader, antenna, Uninterruptible Power Supply (UPS), communication lines, equipment enclosure, and related equipment installation mounts and hardware will be inspected to ensure proper operation.

ATTACHMENT B
PAYMENT/COMPENSATION

1. **Compensation:** This is a firm-fixed fee Contract between the County and Contractor for Hardware and Software Maintenance Services as set forth in Attachment A, "Scope of Work".

   The 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 the Contractor of all its duties and obligations hereunder. The Contractor shall only be compensated as set forth herein for work performed in accordance with the Scope of Work. **The 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 C and P of the County Contract Terms and Conditions.**

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

Maintenance Period	Annual Hardware and Software Maintenance and Support
9/1/2026 through 8/31/2027	$91,292.00
9/1/2027 through 8/31/2028	$94,935.00
9/1/2028 through 8/31/2029	$98,726.00
9/1/2029 through 8/31/2030	$102,668.00
9/1/2030 through 8/31/2031	$106,769.00

   Total Contract Amount Not To Exceed: $494,390.00

3. **Price Increase/Decreases:** No price increases will be permitted during the term of the Contract. The 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 to secure such adjustment. No retroactive price adjustments will be considered. All price decreases will automatically be extended to the County of Orange. The 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 the Contract. Adjustments increasing the 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 the County du ring the term of this Contract not otherwise specified and provided for within this Contract.

5. **Contractor's Expense:** The Contractor will be responsible for all costs related to photo copying, telephone communications and fax communications, and parking 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. Vendor shall reference Contract number on invoice. Payment will be net 30 days after receipt of an invoice in a format acceptable to the 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 the Contractor.

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

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

7. **Taxpayer ID Number:** The Contractor shall include its taxpayer ID number on all invoices submitted to the County for payment to ensure compliance with IRS requirements and to expedite payment processing.

8. **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 1 above
   C. Contractor's Federal Taxpayer ID Number
   D. Name of County Agency/Department
   E. Delivery/service address
   F. Master Agreement MA-280-26011292
   G. Agency/Department's Account Number
   H. Date of invoice and invoice number
   I. Product/service description, quantity, and prices
   J. Order Date/Service Date(s)
   K. Sales tax, if applicable
   L. Freight/delivery charges, if applicable
   M. Total

   Invoices and support documentation are to be forwarded to **(not both):**

   Mailed to John Wayne Airport
   Attention: Accounts Payable
   3160 Airway Avenue
   Costa Mesa, CA 92626

   OR

   Emailed to AccountsPayable@ocair.com

   Contractor has 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 Electronic Remittance Advice with the payment details via email. An email address will need to be provided to the County via and EFT Authorization Form. To request a form, please contact the DPA.

ATTACHMENT C
COUNTY OF ORANGE INFORMATION TECHNOLOGY SECURITY GUIDELINES
(SEPARATE ATTACHMENT)

ATTACHMENT D
KEY PERSONNEL/STAFFING PLAN

1) **Key Personnel**

Name	Classification/Designation	Years of Experience	Years with Company	Professional License or Credentials
John Azevedo	Principal Engineer, Airport Systems and Services	35	17	Electrical Engineering
Mark Cox	Sr. System Engineer	32	32	Electrical Engineering

Contractor understands that the individuals represented as assigned to the Contract must remain working on the Contract throughout the duration of the Contract unless otherwise requested or approved by County. Substitution of Contractor's Key Personnel shall be allowed only with prior written approval of County's Project Manager.

Contractor may reserve the right to involve other Contractor personnel, as their services are required. The specific individuals will be assigned based on the need and timing of the service/classification required. Assignment of additional key personnel shall be subject to County written approval. County reserves the right to have any of Contractor personnel removed from providing services to County under this Contract. County is not required to provide any reason for the request for removal of any Contractor personnel.

2) **Subcontractor(s)**

Listed below are subcontractor(s) anticipated by Contractor to perform services specified in Attachment A. Substitution or addition of Contractor's subcontractors in any given project function shall be allowed only with prior written approval of County's Project Manager.

Company Name & Address	Contact Name and Telephone Number	Project Function
GateKeeper Systems, Inc 880 Blue Gentian Road Suite 140 Eagan, MN 55121	Anne Turner 651-365-0700	Provide software services and support for GateKeeper CVMS, which is the Ground Transportation Management software utilized by the GT staff at SNA.

ATTACHMENT E
GSI - CYBER SECURITY ENHANCEMENTS
(SEPARATE ATTACHMENT)

ATTACHMENT F
SNA - SOFTWARE MAINTENANCE AGREEMENT WITH ADCOMP – 2026
(SEPARATE ATTACHMENT)

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.

880 Blue Gentian Road
Suite 140
Eagan, MN 55121

Phone (651) 365-0700
Fax (651) 365-0777
www.gksys.com

Support Renewal 2026 - Attachment A

Support costs reflect ongoing cyber security enhancements to the GateKeeper CVMS software. These enhancements are necessary as we continue to prioritize the security and efficiency of our system. As a part of these efforts Single Sign On (SSO) was introduced with version 8.5+ and will now be part of the GateKeeper CVMS package.

• **Enhanced Security**: With the growing complexity of cyber threats, an upgraded SSO solution offers a critical layer of protection. By consolidating authentication mechanisms into a centralized platform, we reduce the risk of weak or repeated passwords, implement multifactor authentication (MFA), and ensure compliance with industry security standards.

• **Improved User Experience**: SSO enables employees to access all authorized applications with a single set of credentials, streamlining workflows and enhancing productivity. Reducing the number of logins required for each application minimizes both frustration and the number of support tickets related to password resets, providing a smoother experience for end-users.

• **Operational Efficiency and Cost Savings**: SSO can reduce the time spent by IT or admin teams managing password-related issues, allowing them to focus on more strategic initiatives.

880 Blue e Ro d
Su te 140
g an, MN 55121

Pho e (651) 365-0700
F x (651) 365-0777
www.gksys.com

SOFTWARE MAI T A CE AGREEMENT

General Description

Under this agreement, G eKeeper Systems, Inc. (GSI) will maint good work g order he computer sof ware lice sed o John Wayne In ernatio l Airport (the Airpor) and known as the GateKeeper Systems Commercial Veh cle Management (CVM) sof ware, nd other related sof ware compo ents supplied by GateKeeper Systems.

Covered Software

1. eKeeper Commerc l Vehicle M geme (CVM) sof w re
2. eKeeper Vendor Website
3. TNC-Ops™ Module
4. F c l Module (Adcomp software)
5. Software Mo itor g

Software Support Services

eKeeper Systems, l c. will provide sof w re suppor to Airport personnel as ecessary o elim e or correct software malfunctio s and return the software to normal oper o n. The categories of softw re suppor o be prov ded under h s co r c clude:

1. Response to System Problems: ateKeeper Systems will provide o -line and elephone suppor to A rport perso el as eeded for the period of the co rac to remotely d g ose and make requ red changes to the *Covered So re* l sted above. Suppor will be prov ded by qualified GSI perso el familiar with the Commercial Veh cle Man gement system d software installed at the A rport.

2. System Mo oring: GateKeeper Systems will perform ongoing checks o system components and eKeeper CVMS software - utilizing co nfigurable mo oring and lerti g tool. For th s sof ware to be effective. GateKeeper will prov de an SMTP mail rel y for Ga eKeeper software to use for sending out alerts, scheduled tasks, password rese s etc. Addit o lly, GateKeeper Sys ems alarm mon toring requires a secure webservice co ec on that must be open for complete monitor g service. GateKeeper Systems will co c the ppropriate Airpor staff o coordinate the completio of ny required items should they i erfere with operatio s.

3. System Updates: The Airport will inst ll "Cr c l Upda es" for the Microsoft operating d SQL da base systems as specified by the Airport ernal process requ rements. The Airport is respo s ble for install on of service packs on the productio servers. GateKeeper Systems will work with the Airpor d provide appropri e recommend ons for schedul g and install o i he produc on e v ronme .

4. System Upgrade: This Software Maintenance Agreeme cludes a fully paid license for ew versions of the CVMS sof w re that is rele sed during the term of h s agreement. The Airport is no required to impleme ll versions of the software. Upgr de implementatio costs are covered for up to one upgrade per year. New versions of the Covered Sof w re may require OS or SQL software upgrades as minimum d ba se and server requireme s change over time. Ga eKeeper's effort to support server operati g sys em and/or database upgrades may cur add o al cos .

5. AdComp Serv ces: GateKeeper Systems (and AdComp) will provide on-l e telepho e d email support for the TAMS dmin stratio and vendor p yment portal sof ware and services. Th s cludes the payment gateway service fees.

Period of Coverage

Telephone support is available 24 hours per day and 7 days per week for the period of the agreement.

Support Request Procedure

The Airport sh ll ide fy wri g at the o n of the contract, personnel authorized to request software assistance. When ssistance is requ red, the d v du l respo sible should call GateKeeper Systems as follows:

GateKeeper Emergency Support: (866) 688-3404

This number should be used for support issues th need immediate resolu ion. Th s number is nswered 24 hours per day, 365 days per ye r. If the support spec l st nswering the pho e ca ot address he problem, he oper or w ll record nform o bout the request or problem and immed ely co c he best av lable GSI spec l st to respo d.

GateKeeper Non-Emergency Support: (651) 365-0700

Th s number should be used during normal business hours for issues or questions that do not need immed e resolu on to maintain sys em operatio .

E-mail messages may be se to Suppor @gksys.com for on-emergency requests for support and formati o . I is understood these no -emergency requests are o mo nitored on weekends, holidays or after normal business hours.

Response Time

eKeeper Systems, Inc. will respond to issues immed ely dur g n ormal working hours (8:00 am to 5:00 p.m. Mo day through Friday local Minneapol s time).

Out of normal worki g hours (nigh s, weekends, holid ys, etc.) GateKeeper will respo d to no - emerge cy i ems o the next bus ess day. For emergency calls, qu alified suppor specialist will respond w h 1.5 hours.

Access

Software Ma e ance is co d o ed upon provis o by the A rport to ateKeeper of reaso ble appropriate access to the system(s) running the Covered Software, including, bu not limited to, passwords, system d , file transfer cap bilities, and remote log-in-capab lities. GateKeeper w ll maintain security of the system and use such access only for he purposes of this Agreement d will comply with Client's s dard security procedures.

Owner Responsibilities

A rport perso nel making a request for ssistance should be prepared to provide detailed informatio regarding the problem experienced c ons already ke to remedy the problem and curren operating condition of the software and entire system.

I add on, the Airport agrees to provide, at its expense, remo e access to the system via a secure e work co ect on for d g os s a d/or softw re modif c ons to the system. Airpor personnel maki g the phone request should be prepared to work wi h GSI perso el as ecessary for he durat on of the pho e call.

xclusions

- On-s e software support
- Repair of servers
- Repair of owner provided LAN/WAN equ pment
- Server OS and SQL da base licensing and upgrades
- Formal raining o her ha what is specifically covered in this agreement

Additional Services

Software:

From time to time the Airpor may den fy, through pho e consultatio s or by o her means, the need o mod fy or change the sof ware to eliminate the future occurrence of a problem or o change the method of oper o . TransCore will provide writ en est m e or quote for making the desired changes for approval outside of th s agreement.

Contract Summary Form

OC Expediter Requisition #: 1791563

TRANSCORE LP

10600 Vista Sorrento Parkway, Suite 410

San Diego, CA 92121

SUMMARY OF SIGNIFICANT CHANGES

N/A

SUBCONTRACTORS

This contract includes the following subcontractors or pass through to other providers.

Subcontractor Name	Service(s)	Amount
GateKeeper Systems, Inc.	Commercial Vehicle Management System software, secure portal, TNC/Ride App. module.	Unknown at this time
AdComp Systems Group	Payment processing, invoicing, tracking software.	Unknown at this time

CONTRACT OPERATING EXPENSES

Total Contract Amount Not to Exceed: $494,390