CONTRACT MA-280-23011171

FOR

PARCS MAINTENANCE AND REPAIR

BETWEEN

COUNTY OF ORANGE, JOHN WAYNE AIRPORT

AND

SKIDATA, INC.

JOHN WAYNE AIRPORT
ORANGE COUNTY

CONTRACT MA-280-23011171
FOR
PARCS MAINTENANCE AND REPAIR
BETWEEN
COUNTY OF ORANGE, JOHN WAYNE AIRPORT
AND
SKIDATA, INC.

This Agreement ("Contract") for PARCS Maintenance and Repair 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, through its department John Wayne Airport (hereinafter referred to as "County" or "JWA") and SKIDATA, Inc., with a place of business at 16600 Sherman Way Ste 150, Van Nuys, CA 91406-3792 (hereinafter referred to as "Contractor"), with County and Contractor sometimes referred to as "Party" or collectively referred to 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 – Contractor's Pricing
Attachment C - County of Orange Information Technology Security Standards
Attachment D – Staffing Plan
Attachment E – John Wayne Airport – IT Change Request Form
Attachment F – Schedule of Deductions
Attachment G – Out-Of-Scope Non-Covered Parts Pricing
Attachment H – SKIDATA Responsibility Matrix

RECITALS

WHEREAS, Contractor and County are entering into this Contract for PARCS Maintenance and Repair under a firm fixed rate Contract; and,

WHEREAS, County solicited Contract for PARCS Maintenance and Repair as set forth herein, and Contractor represented that it is qualified to provide PARCS Maintenance and Repair to the County as further set forth here; and,

WHEREAS, Contractor agrees to provide PARCS Maintenance and Repair to the County as further set forth in the Scope of Work, attached hereto as Attachment A and incorporated herein; and

WHEREAS, County agrees to pay Contractor the fees as set forth in Contractor's Pricing, attached hereto as Attachment B and incorporated herein;

WHEREAS, the County Board of Supervisors has authorized the Deputy Purchasing Agent or designee to enter into a Contract for PARCS Maintenance and Repair with the Contractor;

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

DEFINITIONS

DPA shall mean the Deputy Purchasing 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. SKIDATA is not authorized by the manufacturers of the equipment, the Software, and any replacement parts, to make any warranties on their behalf. 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. **Non-Discrimination:** In the performance of this Contract, Contractor agrees that it will comply with the requirements of Section 1735 of the California Labor Code and not engage nor permit any subcontractors to engage in discrimination in employment of persons because of the race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, marital status, or sex of such persons. Contractor acknowledges that a violation of this provision shall subject Contractor to penalties pursuant to Section 1741 of the California Labor Code.

a. **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:

1. **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.

2. **Nondiscrimination:** The Contractor, with regard to the work performed by it during the contract, will not discriminate on the grounds of race, color, or national origin 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.

3. **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.

4. **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.

5. **Sanctions for Noncompliance:** In the event of a Contractor's noncompliance with the non-discrimination 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.

6. **Incorporation of Provisions:** The Contractor will include the provisions of paragraphs one through six 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.

b. **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 non-discrimination statutes and authorities; including but not limited to:

1. 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);

2. 49 CFR part 21 (Non-discrimination in Federally-assisted programs of the Department of Transportation—Effectuation of Title VI of the Civil Rights Act of 1964);

3. 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);

4. 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;

5. The Age Discrimination Act of 1975, as amended (42 USC § 6101 *et seq*.) (prohibits discrimination on the basis of age);

6. Airport and Airway Improvement Act of 1982 (49 USC § 471, Section 47123), as amended (prohibits discrimination based on race, creed, color, national origin, or sex);

7. The Civil Rights Restoration Act of 1987 (PL 100-209) (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);

8. Titles II and III of the Americans with Disabilities Act of 1990, which 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 (42 USC §§ 12131 – 12189) as implemented by U.S. Department of Transportation regulations at 49 CFR parts 37 and 38;

9. The Federal Aviation Administration's Nondiscrimination statute (49 USC § 47123) (prohibits discrimination on the basis of race, color, national origin, and sex);

10. Executive Order 12898, Federal Actions to Address Environmental Justice in Minority Populations and Low-Income Populations, which ensures nondiscrimination against minority populations by discouraging programs, policies, and activities with disproportionately high and adverse human health or environmental effects on minority and low-income populations;

11. Executive Order 13166, Improving Access to Services for Persons with Limited English Proficiency, and resulting agency guidance, national origin discrimination includes discrimination because of limited English proficiency (LEP). To ensure compliance with Title VI, you must take reasonable steps to ensure that LEP persons have meaningful access to your programs (70 Fed. Reg. at 74087 to 74100);

12. 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).

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 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 carryall 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 (SIRs) shall be clearly stated on the Certificate of Insurance. Any SIRs 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 00 12, 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.

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.

If Contractor's Professional Liability, Technology Errors & Omissions and/or Network Security & Privacy Liability are "Claims-Made" policy(ies), Contractor shall agree to the following:

1) The retroactive date must be shown and must be before the date of the Contract or the beginning of the Contract services.

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

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

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 agree 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.

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 third party 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 make available 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 Purchasing 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.

Additional Terms and Conditions:

1. **Scope of Contract:** This Contract specifies the contractual terms and conditions by which the County will procure PARCS Maintenance and Repair 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 August 1, 2023 and shall continue for three (3) year(s), unless otherwise terminated as provided herein. This Contract may be renewed as set forth in paragraph 3 below.

3. **Renewal:** This Contract may be renewed by mutual written agreement of both Parties for One (1) additional two (2) year term. The County does not have to give reason if it elects not to renew. Renewal periods may be subject to approval by the County of Orange Board of Supervisors.

4. **Contract Amount not to exceed:** Contract Amount not to exceed **$2,257,644.**

Year 1	Year 2	Year 3
$ 740,352	$ 749,359	$ 767,933

5. **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 (7) 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 Purchasing 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.

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

7. **Airport Security:** If it is determined by the Airport that a Contractor, Contractor's employees and/or Contractor's subcontractors have an operational need to have unescorted access to restricted areas of the Airport or remote access to critical Airport systems, the following must be completed in order to obtain an Airport-Issued Security Identification Badge (ID Badge).

   A. Physical Access

      i. **Airport-Issued Badge Acquisition, Retention, and Termination**: Prior to issuance of airport security ID Badge(s), designated Contractor personnel who shall be working on-site in JWA restricted areas, and engaged in the performance of work under this Contract must pass JWA's security background screening requirements, which include fingerprinting to complete an F.B.I. Criminal History Records Check (CHRC) and a Security Threat Assessment (STA). Contractor should anticipate four to six weeks for new employees to receive an airport security ID badge which includes the following general steps:

         1. Company designates at least two representatives as Authorized Signatories by submitting a letter on company letterhead using the airport's template.
         2. Subcontractors and tenant contractors must also have two Authorized Signatories at a minimum.
         3. All company employees requiring unescorted access to restricted airport areas are scheduled for fingerprint appointments.
         4. Background check fees are provided at the first appointment.
         5. Employees must provide two government-issued IDs at the first appointment.
         6. STA and/or CHRC results are received.
         7. All ID Badge applicants successfully passing the STA and/or CHRC are scheduled for required training.
         8. ID Badge related fees are provided and any additional information requested is provided at the training appointment.
         9. Upon successful completion of the required training, employees will receive their ID Badge.
         10. Authorized Signatories are required to maintain the ID Badge process for the onboarding of future employees, employee ID Badge renewals, scheduling, and other actions detailed below.

      ii. Contractor's designated personnel must, at a minimum, complete the following required training based on contractors work to be provided and access areas:

         1. Authorized Signatory Training: All organizations must designate at least two Authorized Signatories by providing a letter on company letterhead using the ID/Access Control Office template. The designated Authorized Signatories will be responsible for the entire ID Badge process for their organization including, but not limited to, the onboarding of new employees, renewing employees, scheduling employees for appointments, payment coordination, ID Badge audits, resolution to safety/security violations caused by the organizations employees, subtenants, or subcontractors. Authorized Signatories must attend this approximate 1 hour course initially and annually.

         2. Security Identification Display Area (SIDA) Training: All employees with an operational need to have unescorted access to the Airport SIDA must complete this approximate 1.5 hour course and pass a written test.

3. Sterile Area (Elevator) Training: All Non-SIDA employees with an operational need to have unescorted access to the Sterile Area of the terminal must complete an approximate 30-minute training session and pass a written test.
4. Non-Movement Area or Movement Area Driver Training: All employees with an operational need to drive on airfield service roads and/or ramps must attend the approximate 1-hour Non-Movement Area Driver course and pass a written test. Employees with an operational need to drive on active taxiways and/or active runways must coordinate this training with the Airport Operations Division.
5. Contractors' designated personnel must successfully complete the badge acquisition within six weeks of Contract execution, unless other arrangements have been coordinated by County Project Manager or designee in writing.
6. All personnel assigned to this contract must be in possession of a current, valid Airport-Issued ID Badge prior to fulfilling an independent shift assignment.
7. Contractor is responsible for terminating and retrieving Airport-Issued ID Badges as soon as an employee no longer needs unescorted access to airport restricted areas. Terminated ID Badges must be returned to the ID/Access Control office within three business days. Failure to do so will result in a $250.00 fee.
8. Contractor shall be responsible for all cost associated with the Airport-Issued ID Badge process The ID/Access Control Office maintains the current list of fees. Below is a list of estimated costs for new ID Badge applications and ID Badge renewals:
    - STA Fee: Approximately $11.00
    - Fingerprint/CHRC Fee: Approximately $31.00
    - ID Badge Fee: Approximately $10.00
    - Terminated, Unreturned ID Badge Fee: Approximately $250.00
9. Contractor shall abide by all the security requirements set forth by the Transportation Security Administration (TSA) and JWA.

iii. **Airside Driving Endorsement:** In addition to obtaining a JWA access control badge, Contractor's service staff with an operational need to drive on airport service roads and ramps must also take an Airport provided training course and pass a test to acquire an airfield driving endorsement.

Some Air Operations Area projects will require vehicles to be equipped with visible company placards on both sides of the vehicle, an orange/white checkered flag, an amber, rotating beacon, and a two-way radio to monitor FAA Air Traffic Control Tower frequencies; or be escorted by a vehicle with this equipment and markings. Only vehicles, equipment, and personnel who have prior authorization by the ASP may operate on runways, taxiways and movement areas, or cross runways and taxiways. Under no circumstances shall any vehicle operate on or cross a runway, taxiway, or any movement area unless permission from the Tower is granted. Vehicles requiring an escort must be escorted by Airport Operations, or authorized company vehicles, equipped with two-way radios, and in constant radio communication with the FAA Control Tower.

iv. **Airport ID Badge Holder Requirements and Responsibilities:** TSA approved security program for JWA requires that each person issued a JWA security badge is made aware of his/her responsibilities regarding the privilege of access to restricted areas of JWA.

1. All persons within the restricted air operation areas of JWA are required to display, on their person, a JWA security badge; unless they are specifically exempted for safety reasons or they are under escort by a properly badged individual. Each JWA employee, JWA Contractor,

subcontractor or tenant employee who has been issued a JWA security badge is responsible for challenging any individual who is not properly displaying a JWA issued or approved and valid identification badge. Any person who is not properly displaying or who cannot produce a valid JWA security badge must immediately be referred to the Sheriff's Department - Airport Police Services Office for proper handling.

2. JWA security badge is the property of County and must be returned upon termination of Contractor personnel employment and/or termination, expiration or completion of Contract. The loss of a badge shall be reported within 24 hours to the Sheriff's Department - Airport Police Services by calling (949) 252-5000. Individuals that lose their badge shall be required to pay a fee before receiving a replacement badge. The charge for lost badge replacement shall be at the current posted rate located in the JWA Administration Office. A report shall be made before a replacement badge shall be issued.
3. JWA security badge is nontransferable.
4. In the event that a contractor's badge is not returned to JWA upon termination of Contractor personnel employment and/or termination or expiration of Contract, a fine of $250.00 per badge shall be charged to Contractor. Contractor's final payment may be held by County or a deduction from contractor's payment(s) may be made to ensure that funding is available to cover the fine in the event that badges are not returned.
5. Contractor shall submit the names, addresses, and driver's license numbers for all Contractor personnel who shall be engaged in work under this Contract to County Project Manager within seven days after award of the Contract or within seven days after the start of any new Contractor personnel and/or prior to the start of any work.
6. No worker shall be used in performance of this work that has not passed the background check.

B. Remote or Physical Access to Critical Airport Systems:

i. Contractor, Contractor's employees, and subcontractors who do not need unescorted access to restricted Airport areas may be required by JWA to complete and pass security background screening requirements if their performance of work under this contract meets certain criteria, including but not limited to:

1. Employee will be required to be on-site on a routine or recurring basis in the daily performance of their duties or to complete a temporary or long-term project.
2. Employee will not be on-site but will connect remotely to JWA systems through an unescorted or escorted remote access mechanism.
3. Employee will have access to JWA data or systems that are deemed sensitive or require a high level of security due to mandate, law, or policy.

8. **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.

9. **Bills and Liens:** Contractor shall pay promptly all indebtedness for labor, materials and equipment used in performance of the work. Contractor shall not permit any lien or charge to attach to the work or the premises, but if any does so attach, Contractor shall promptly procure its release and, in accordance with the

requirements of paragraph "Z" above, indemnify, defend, and hold County harmless and be responsible for payment of all costs, damages, penalties and expenses related to or arising from or related thereto.

10. **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.

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

    The Contractor agrees to comply with pertinent statutes, Executive Orders and such rules as are promulgated to ensure that no person shall, on the grounds of race, creed, color, national origin, sex, age, or disability be excluded from participating in any activity conducted with or benefiting from Federal assistance.

    This provision binds the Contractor and subcontractors from the bid solicitation period through the completion of the contract. This provision is in addition to that required by Title VI of the Civil Rights Act of 1964.

12. **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. County of Orange Information Technology Security Standards: County of Orange security standards follows the latest National Institute of Standards and Technology (e.g. 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 Standards ("Security Standards"), as existing

or modified, that pertain to Contractor in connection with the Services performed by Contractor as set forth in the scope of work of this Contract. Any violations of such Security Standards shall, in addition to all other available rights and remedies available to County, be cause for immediate termination of this Contract. Such Security Standards include, but are not limited to, Attachment C - County of Orange Information Technology Security Standards.

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

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 (e.g. 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) 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.

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 (e.g. 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.

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 uncured 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. Upon receiving written notice of any security failures, Contractor shall be afforded a thirty (30) day cure period. 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 72 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:

Ed Althof

Linda Le, CHPC, CHC, CHP

Interim Chief Information Security Officer
1055 N. Main St., 6th Floor
Santa Ana, CA 92701
Phone: (714) 834-3069
Ed.Althof@ocit.ocgov.com

County Privacy Officer
1055 N. Main St., 6th Floor
Santa Ana, CA 92701
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.

J. 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.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 an 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.

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

14. **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.

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

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

17. **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 time lines. 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.

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

19. **Contractor Personnel – Uniform/Badges/Identification:** The Contractor warrants that all persons employed to provide service under this Contract have satisfactory past work records indicating their ability to accept the kind of responsibility under this Contract.

All Contractor's employees shall be required to wear uniforms, badges, or other means of identification which are to be furnished by the Contractor and must be work at all times while working on County property. The assigned Deputy Purchasing Agent must be notified in writing, within seven (7) days of notification of award of Contract of the uniform and/or badges and/or other identification to be worn by employees prior to beginning work and notified in writing seven (7) days prior to any changes in this procedure.

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

21. **Cooperative Contract:** This Contract is a cooperative contract and may be utilized by all County of Orange Departments.

    The provisions and pricing of this Contract will be extended to other governmental entities. Governmental entities wishing to use this Contract will be responsible for issuing their own purchase documents, providing for their own acceptance, and making any subsequent payments. Contractor shall be required to include in any subordinate contract entered into with another governmental entity pursuant to this Contract, a contract clause that will hold harmless the County of Orange from all claims, demands, actions or causes of actions of every kind resulting directly or indirectly, arising out of, or in any way connected with the use of this Contract. Failure to do so will be considered a material breach of this Contract and grounds for immediate Contract termination. Governmental entities are responsible for obtaining all certificates of insurance, endorsements and bonds required. The Parties agree that any other governmental entity utilizing this Contract shall not be deemed to be an agent or employee of County for any purpose whatsoever. The Contractor is responsible for providing each governmental entity a copy of this Contract upon request. The County of Orange makes no guarantee of usage by other users of this Contract.

    The Contractor shall be required to maintain a list of the County of Orange departments and governmental entities using this Contract. The list shall report dollar volumes spent annually and shall be provided on an annual basis to the County, at the County's request.

    Subordinate contracts must be executed prior to the expiration or earlier termination of this Contract and may survive the expiration of this Contract up to a maximum of one year; however, in no case shall a subordinate contract exceed five (5) years in duration.

22. **County Branding Requirement – Publicity, Literature, Advertisements and Social Media:**

    A. County owns all rights to the name, logos, and symbols of County. The use/and/or reproduction of County's name, logos, or symbols for any purpose, including commercial advertisement, promotional purposes, announcements, displays, or press releases, without County's prior written consent is expressly prohibited.

    B. Contractor may develop and publish information related to this Contract where all of the following conditions are satisfied:

        1) Administrator/assigned Deputy Purchasing Agent provides its written approval of the content and publication of the information at least 30 days prior to Contractor publishing the information, unless a different timeframe for approval is agreed upon to the Administrator/assigned Deputy Purchasing Agent;

2) Unless directed otherwise by Administrator/assigned Deputy Purchasing Agent, the information includes a statement that the program, wholly or in part, is funded through County, State and Federal government funds [funds identified as applicable];

3) The information does not give the appearance that the County, its officers, or employees or agencies endorse:

   i. any commercial product or service; and,
   ii. any product or service provided by Contractor, unless approved in writing by Administrator/assigned Deputy Purchasing Agent; and,

4) If Contractor uses social media (such as Facebook, Twitter, YouTube or other publicly available social media sites) to publish information related to this Contract, Contractor shall develop social media policies and procedures and have them available to the Administrator/assigned Deputy Purchasing Agent. Contractor shall comply with County Social Media Use Policy and Procedures as they pertain to any social media developed in support of the services described within this Contract. The policy is available on the Internet at http://www.ocgov.com/gov/ceo/cio/govpolicies.

23. **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.

24. **Default – Equipment, Software or Service:** In the event any equipment, software or service furnished by the Contractor in the performance of this Contract should fail to conform to the specifications therein, the County may reject same, and it shall become the duty of the Contractor to reclaim and remove the items without expense to the County and to immediately replace all such rejected equipment, software or service with others conforming to such specifications, provided that should the Contractor fail, neglect or refuse to do so, the County shall have the right to purchase on the open market a corresponding quantity of any such equipment, software or service and to deduct from any monies due or that may thereafter become due to the Contractor the difference between the price specified in this Contract and the actual cost to the County.

    In the event the Contractor shall fail to make prompt delivery as specified of any equipment, software or service, the same conditions as to the rights of the County to purchase on the open market and to reimbursement set forth above shall apply, except as otherwise provided in this Contract.

    In the event of the cancellation of this Contract, either in whole or in part, by reason of the default or breach by the Contractor, any loss or damage sustained by the County in procuring any equipment, software or service which the Contractor agreed to supply under this Contract shall be borne and paid for by the Contractor.

    The rights and remedies of the County provided above shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Contract.

25. **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.**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 Purchasing Agent by way of the following process:

A. The Contractor shall submit to the agency/department assigned Deputy Purchasing Agent a written demand for a final decision regarding the disposition of any dispute between the parties arising under, related to, or involving this Contract, unless 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 Purchasing Agent or his designee. . 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.

26. **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.

27. **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.

28. **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.

29. **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, colornational 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.

30. **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.

31. **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.

32. **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

33. **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.

34. **Hazardous Conditions:** Whenever the Contractor's operations create a condition hazardous to traffic or to the public, the Contractor shall provide flagmen and furnish, erect and maintain control devices as are necessary to prevent accidents or damage or injury to the public at Contractor's expense and without cost to the County. The Contractor shall comply with County directives regarding potential hazards.

    Emergency lights and traffic cones must also be readily available at all times and must be used in any hazardous condition. Emergency traffic cones must be placed in front of and behind vehicles to warn oncoming traffic.

    Signs, lights, flags, and other warning and safety devices shall conform to the requirements set forth in Chapter 6 of the current traffic manual, Traffic Control for Construction and Maintenance Work Zones, published by the state of California Department of Transportation.

35. **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**.**

36. **Inventions:** If any discovery or invention arises or is developed in the course of, or as a result of work performed under this Contract, the Contractor shall refer the discovery or invention to the County.

37. **Material, Workmanship, and Acceptance:** All Materials furnished by Contractor in the work shall be new, high-grade, and free from defects. Quality of work shall be in accord with the general accepted standards. Materials, parts, equipment and work quality shall be subject to County's approval.

    Materials and work quality not conforming to the requirement of the Scope of Work shall be considered defective and shall be subject to rejection. Defective work or material, whether in place or not, shall be removed immediately from the site by Contractor, at its expense, when so directed by County.

    If Contractor fails to replace any defective or damaged work or material within 72 hours after notice, Contractor agrees to provide a workaround within 24 hours as specified in Section 16 Scope of Work, Exhibit A. County may cause such work or materials to be replaced. Replacement expense shall be deducted from the amount to be paid to Contractor.

    Where materials are specified by reference to standard specifications of the American Society for Testing Materials (ASTM), American National Standards Institute (ANSI), Builders Hardware Manufacturers Association (BHMA), Federal Specifications, or others, all applicable provisions of the designated specifications shall be considered as forming a part of the Contract documents to the same force and effect as if repeated therein.

38. **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.

39. **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 Purchasing 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:	SKIDATA, Inc. Attn: Mary Beth Mcnair 16600 Sherman Way Ste 150 Van Nuys, CA 91406-3792 Phone: (818) 429-7362 Email: marybeth.mcnair@skidata.com
County's Project Manager:	JWA/Information Technology (Operations) Attn: William Bogdan, Admin Manager II 3160 Airway Ave. Costa Mesa, CA 92626 Phone: (949) 255-1336 Email: wbogdan@ocair.com
cc:	JWA/Procurement Attn: Thang Bernard, County DPA 3160 Airway Avenue Costa Mesa, CA 92626 Phone: (949) 252-6074 Email: tbernard@ocair.com

40. **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.

41. **Order Dates:** Orders may be placed during the term of the Contract even if delivery may not be made until after the term of the Contract. The Contractor must clearly identify the order date on all invoices to County and the order date must precede the expiration date of the Contract.

42. **Ownership of Documents:** The County has permanent ownership of all directly connected and derivative materials produced under this Contract by the Contractor. All documents, reports and other incidental or derivative work or materials furnished hereunder shall become and remain the sole property of the County and may be used by the County as it may require without additional cost to the County. None of the documents, reports and other incidental or derivative work or furnished materials shall be used by the Contractor without the express written consent of the County. Contractor retains all right, title and interest in any pre-existing intellectual property which may be used in performing the Services, including any modifications or improvements made during the performance of the Services (Contractor Property). To the extent Contractor Property is embodied in any deliverable, Consultant grants County a worldwide, non-exclusive, royalty-free, perpetual, non-sublicensable, license to use Contractors Property for County's general business purpose solely with respect to such deliverable.

43. **Payment Card Industry Data Security Data Standard:** Contractor covenants and warrants that it is currently PCI DSS compliant and will remain compliant during the entire duration of this Contract. Contractor agrees to immediately notify County in the event Contractor should ever become non-compliant, and will take all necessary steps to return to compliance and shall be compliant within ten (10) days of the commencement of any such interruption.

    Upon demand by County, Contractor shall provide to County written certification of Contractor's PCI/DSS and/or PA DSS compliance.

44. **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.

45. **Prevailing Wage:**

    a. Threshold Requirements for Prevailing Wages: Except for public works project of one thousand dollars ($1,000) or less, not less than the general prevailing rate of per diem wages for work of a similar in character in the locality in which the public work is performed, and not less than the general prevailing rate of per diem wages for holiday and overtime work fixed as provide in this chapter, shall be paid to all workers employed on a public works.

    b. Wage Rates: Contractor shall post a copy of the wage rates at the job site and shall pay the adopted prevailing wage rates as a minimum. Pursuant to the provisions of Section 1773 of the Labor Code of the State of California, the Board of Supervisors has obtained the general prevailing rate of per diem wages and the general prevailing rate for holiday and overtime work in this locality for each craft, classification, or type of workman needed to execute this Contract from the Director of the Department of Industrial Relations. These rates are on file with the Clerk of the Board of Supervisors. Copies may be obtained at cost at the office of County's OC Public Works/OC Facilities & Asset Management/A&E Project Management or visit the website of the Department of Industrial Relations, Prevailing Wage Unit at www.dir.ca.gov/DLSR/PWD. The Contractor shall comply with the provisions of Sections 1774, 1775, 1776 and 1813 of the Labor Code.

    c. Apprenticeship Requirements: The Contractor shall comply with Section 230.1(A), California Code of Regulations as required by the Department of Industrial Relations, Division of Apprenticeship Standards by submitting DAS Form to the Joint Apprenticeship Committee of the craft or trade in the area of the site.

    d. Registration of Contractor: All Contractors and Subcontractors must comply with the requirements of Labor Code Section 1771.1(a), pertaining to registration of contractors pursuant to Section 1725.5. Bids cannot be accepted from unregistered contractors except as provided in Section 1771.1. This project is subject to compliance monitoring and enforcement by the Department of Industrial Relations. After award of the contract, Contractor and each Subcontractor shall furnish electronic payroll records directly to the Labor Commissioner in the manner specified in Labor Code Section 1771.4.

    e. Prevailing Wage and DIR Requirement: Awarding agencies are not required to submit the notice of contract award through DIR's PWC-100 system on projects that fall within the small project exemption. The small project exemption applies for all public works projects that do not exceed:

        - $25,000 for new construction, alteration, installation, demolition or repair.

- $15,000 for maintenance.

f. Payroll Records: Contractor and any Subcontractor(s) shall comply with the requirements of Labor Code Section 1776. Such compliance includes the obligation to furnish the records specified in Section 1776 directly to the Labor Commissioner in an electronic format, or other format as specified by the Commissioner, in the manner provided by Labor Code Section 1771.4. The requirements of Labor Code Section 1776 provide, in summary:

i. The information contained in the payroll record is true and correct.

ii. The employer has complied with the requirements of Labor Code Section 1771, 1811, and 1815 for any work performed by his or her employees in connection with the Contract.

iii. The payroll records shall be certified and shall be available for inspection at the principal office of Contractor on the basis set forth in Labor Code Section 1776.

iv. Contractor shall inform County of the location of the payroll records, including the street address, city and county, and shall, within five (5) working days, provide a notice of any change of location and address of the records.

v. Pursuant to Labor Code Section 1776, Contractor and any Subcontractor(s) shall have ten (10) days in which to provide a certified copy of the payroll records subsequent to receipt of a written notice requesting the records described herein. In the event that Contractor or any Subcontractor fails to comply within the 10-day period, he or she shall, as a penalty to County, forfeit $100, or a higher amount as provided by Section 1776, for each calendar day, or portion thereof, for each worker to who the noncompliance pertains, until strict compliance is effectuated. Contractor acknowledges that, without limitation as to other remedies of enforcement available to County, upon the request of the Division of Apprenticeship Standards or the Division of Labor Standards Enforcement of the California Department of Industrial Relations, such penalties shall be withheld from progress payments then due Contractor. Contractor is not subject to penalty assessment pursuant to this section due to the failure of a Subcontractor to comply with this section.

vi. Contractor and any Subcontractor(s) shall comply with the provisions of Labor Code Sections 1771 et seq., and shall pay workers employed on the Contract not less than the general prevailing wage rates of per diem wages and holiday and overtime wages as determined by the Director of Industrial Relations. Contractor shall post a copy of these wage rates at the job site for each craft, classification, or type of worker needed in the performance of this Contract, as well as any additional job site notices required by Labor Code Section 1771.4(b). Copies of these rates are on file at the principal office of County's representative, or may be obtained from the State Office, Department of Industrial Relations ("DIR") or from the DIR's website at www.dire.ca.gov. If the Contract is federally funded, Contractor and any Subcontractor(s) shall not pay less than the higher of these rates or the rates determined by the United States Department of Labor.

g. Work Hour Penalty: Eight (8) hours of labor constitute a legal day's work, and forty hours (40) constitute a legal week's work. Pursuant to Section 1813 of the Labor Code of the State of California, the Contractor shall forfeit to the County Twenty Five Dollars ($25) for each worker employed in the execution of this Contract by the Contractor of by any Subcontractor for each calendar day of during which such worker is required or permitted to work more than the legal day's or weeks' work, except that work performed by employees of said Contractor and Subcontractors in excess of the legal limit shall be permitted without the foregoing penalty upon the payment of compensation to the workers for all hours worked in excess of eight hours per day of not less than 1-12 times the basic rate of pay.

h. Apprentices: The Contractor acknowledges and agrees that, if this Contract involves a dollar amount greater than or a number of working days greater than that specified in Labor Code Section 1777.5, this Contract is governed by the provisions of Labor Code Section 1777.5. It shall be the responsibility of the Contractor to ensure compliance with this Article and with Labor Code Section 1777.5 for all apprenticeable occupations.

Pursuant to Labor Code Section 1777.5 if that Section applies to this Contract as indicated above, the Contractor and any Subcontractors under him employing workers in any apprenticeable craft of trade in performing any work under this Contract shall apply to the applicable joint apprenticeship standards and fixing the ratio of apprentices to journeymen employed in performing the work.

Pursuant to Labor Code Section 1777.5 if that Section applies to this Contract as indicated above, the Contractor and any Subcontractor under him may be required to make contributions to the apprenticeship program.

The Contractor and all Subcontractors under him shall comply with Labor Code Section 1777.6 which Section forbids certain discriminatory practices in the employment of apprentices.

46. **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.

47. **Protection of Restoration of Existing Areas:** Contractor shall be responsible for protection of public and private property adjacent to the work. Contractor shall repair or replace all existing improvements that are damaged or removed as a result of their operation. Repairs and replacements shall be at least equal to existing improvements and shall match them in finish and dimension. All repairs shall be completed with two (2) working days from the date of damage notification unless otherwise approved by County Project Manager.

48. **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 2 hours 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. County agrees to compensate Contractor for any and all costs associated with remediation of emergencies to the extent not caused by Contractor, including but not limited to, expedited shipping, after-hours labor, or rushed processing. 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.

49. **Publication:** No copies of sketches, schedules, written documents, computer based data, photographs, maps or graphs, including graphic art work, resulting from performance or prepared in connection with this Contract, are to be released by Contractor and/or anyone acting under the supervision of Contractor to any

person, partnership, company, corporation, or agency, without prior written approval by the County, except as necessary for the performance of the services of this Contract. All press releases, including graphic display information to be published in newspapers, magazines, etc., are to be administered only by County unless otherwise agreed to by both Parties.

50. **Remedies Not Exclusive:** The remedies for breach set forth in this Contract are cumulative as to one another and as to any other provided by law, rather than exclusive; and the expression of certain remedies in this Contract does not preclude resort by either party to any other remedies provided by law.

51. **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.

52. **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.

53. **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. Nothing in this Agreement requires County to install Updates or Upgrades but Contractor recommends their installation. In case of non-installation of offered Updates or Upgrades, this could possibly endanger the security and operability of software and related systems and may infringe third-party licenses or laws; all consequences of County's rejection of an installation are at the sole risk of the County. Warranty claims regarding systems related to the software will become voidable. The County acknowledges and agrees that Contractor is not liable for damages resulting from the non-installation of Updates and Upgrades.

54. **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.

55. **Software – Inventions, Discoveries, Improvements:** All inventions or discoveries of or improvements to computer programs developed solely pursuant to this Contract shall be the property of the County. Contractor retains all right, title and interest in any pre-existing intellectual property which may be used in performing the ServicesThe 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.

56. **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.

57. **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.

58. **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.

59. **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.

60. **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.

61. **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.

62. **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.

63. **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.

64. **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.

65. **Subcontracting:** No performance of this Contract or any portion thereof may be subcontracted by the Contractor without the express written consent of the County. Any attempt by the Contractor to subcontract any performance of this Contract without the express written consent of the County shall be invalid and shall constitute a breach of this Contract.

    In the event that the Contractor is authorized by the County to subcontract, this Contract shall take precedence over the terms of the Contract between Contractor and subcontractor, and shall incorporate by reference the terms of this Contract. The County shall look to the Contractor for performance and indemnification and not deal directly with any subcontractor. All work performed by a subcontractor must meet the approval of the County of Orange.

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

67. **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 or otherwise provided in writing pursuant to this 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.

68. **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.

69. **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 dates first above written.

SKIDATA, INC.*

Signature	Name	Title	Date
DocuSigned by: 52A7F497F623477...	Robert Weiskopf	Director, Chairman	5/8/2023
DocuSigned by: EDA3A01C80384CB...	David Luken	VP & CEO	5/8/2023

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

Signature	Name	Title	Date
		Deputy Purchasing Agent	

APPROVED AS TO FORM:
County Counsel

By: DocuSigned by: Christine Nguyen 26F9D76C929A49E...
Deputy

Name: Christine Nguyen

Date: 5/8/2023

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

ATTACHMENT A

SCOPE OF WORK

This Contract establishes a maintenance and repair contract between John Wayne Airport ("JWA" or "County") and SKIDATA Control Systems, Inc. ("SKIDATA" or "Contractor") for all systems, equipment, hardware and software known as Parking and Revenue Control System ("PARCS") and License Plate Inventory ("LPI").

The Contract includes Covered Services and parts; and Non-Covered Services and parts; and Systems upgrade; and additional work as outlined below.

I. Contractor Requirements

A. Covered Services and Parts (Monthly Maintenance)

Covered Services includes preventive maintenance, monthly maintenance, replacement of equipment parts, and other activities required to maintain the system.

1. Equipment Services:

Provide maintenance and repair services on the PARCS equipment and License Plate Inventory ("LPI") operated by County at the JWA and related to the installed software & equipment ("System").
Services covered ("Covered Services") under this Services Agreement and included in the ATTACHMENT B CONTRACTOR'S PRICING

2. Equipment Supply and Warranty:

Supply an Extended Warranty following the Manufacturer Warranty Period

All PARCS equipment components, software and hardware listed in "Equipment Covered in Services Agreement" (PARCS Equipment) are warrantied against failure either by manufacturer defect or normal wear and tear ("Extended Warranty"). All-inclusive costs (parts, labor required for repair or replacement of defective PARCS equipment identified in "Equipment Covered in Services Agreement", warranty repairs, shipping charges, travel time, additional expenses relative to Extended Warranty, etc.) incurred during the Extended Warranty Period shall be provided without additional cost to the County.

3. Supply Advanced Replacement of Components:

Contractor will replace all failed components with a serviceable part immediately or with minimal delay from their service inventory to reduce downtime according to the Priority level assigned by the County or Parking Operator to the request, and Repair Time in this Contract below. Failure to do so may result in assessment of penalties in accordance with Attachment F – Schedule of Deductions

Furnish and install all new parts, materials and lubricants which meet or exceed the original equipment manufacturer's specifications. Any parts other than those manufactured by the original equipment manufacturer shall be approved by the County before being incorporated in the work performed by the Contractor under this contract. The Contractor shall maintain a reasonable supply of the parts needed under this contract and maintain a reasonable supply system for the acquisition of additional parts, either immediately or with minimal delay.

B. Preventative Services

Provide Monthly, Quarterly or Annual preventative maintenance, systematic inspection, detection, correction and prevention of incipient failures, including tests, measurements, adjustments, lubrication and labor to replace parts of the equipment including overall inspection of each workstation; ensure hard drives are in working order, verify memory usage and storage capacity.

Provide schedule for preventative maintenance to County for review and approval.

Maintain the PARCS Equipment at a minimum according to manufacturer's recommendations.

C. Software

Provide software maintenance for PARCS Equipment such as but not limited to applicable biannual (semiannual) SKIDATA Software intra-release updates and hotfixes (for supported releases, and as released by the manufacturer) which address reported technical issues, offer applicable feature enhancements or offer improved functionality.

1. Software Updates and Upgrades

Provide the following software updates and upgrades

a. Supplier provided hotfixes to resolve specific JWA issues are within the scope of this contract.

b. SKIDATA labor to install and configure supplier hotfixes to resolve specific JWA issues is within the scope of this contract.

c. Payment Application hotfixes and updates to address PCI compliance requirements per the Secure Implementation Guide based on the latest active PCI DSS standard adopted by JWA. See Payment Card Industry (PCI) PA-DSS Validation Provisions.

d. SKIDATA labor to install and configure Payment Application hotfixes and updates to maintain PCI compliance requirements per the Secure Implementation Guide based on the PCI standards in effect are included. See Payment Card Industry (PCI) PA-DSS Validation Provisions.

e. This specifically includes software, implementation services, and any other costs associated with deployment of a new, revised, enhanced, or modified payment application that may be deemed necessary to meet current PCI DSS validation requirements. See Payment Card Industry (PCI) PA-DSS Validation Provisions.

f. Updates to VMWare, Proventia and Tripwire are included in the scope of this contract.

g. Updates to firmware are included in the scope of this contract.

h. Updates to the server and storage hardware are included in the scope of this contract.

i. With the exception of anti-virus software and Microsoft products mentioned in Payment Card Industry (PCI) PA-DSS Validation Provisions., all other supplier updates, upgrades, or new releases are included from the scope of this contract.

j. SKIDATA labor to install and configure all other supplier updates, upgrades or new releases is excluded from the scope of this contract. Refer to rates specified in Attachment B for labor rates associated with SKIDATA labor to install, configure, test, prepare documentation, provide training to JWA and/or the parking operator, and any other activities associated with these updates and upgrades.

2. Antivirus

Contractor will:

Provide Antivirus maintenance such as manage & regularly verify that antivirus is active, running and latest updates are applied. Review antivirus server and antivirus agents to ensure signatures are up to date and agents are active and functioning.

3. Training

Contractor will:
Provide unlimited customized training for County and County's Parking Operator at the County's request for term of contract. Minimum three (3) attendees per scheduled training is required however every effort will be made to make it economically feasible for both parties.
Topics include but not limited to:

- PARCS equipment
- Preventative maintenance
- SKIDATA reporting

Respond to County request for training within seventy-two (72) hours
Provide a proposed schedule/dates for training to be mutually agreed upon
Provide a proposed agenda for training for County approval no less than five (5) days prior to the mutually agreed to training date and topic. Contractor is to recommend or suggest additional topics to enhance training requested.
Prepare appropriate documentation for training both in hard and soft copy formats for attendees and County if requested.
Provide appropriate trainer for training.
Provide sign-in sheets/ proof of attendance and Certificates of Completion for the training provided to County
Training locations

- Contractor's Training Center located at 6611 Odessa Ave, Van Nuys, CA
- JWA location if requested

4. Help Desk

Contractor will:
Provide access to service help desk during the term of the contract
Provide access to online, real-time access to remote service engineers who are able to launch remote service session to assist with technical issues
Provide a dedicated Account Manager/Project Manager to act as liaison between County and Contractor during the term of the Contract and to direct efforts in fulfilling obligations under this Contract.

SKIDATA's Help Desk can be reached at:

- Phone: 833-SKIDATA (833-754-3282)
- Email: Support.USA@skidata.com
- Online Customer Portal: https://CustomerPortalUSA.skidata.com/

5. Security

Contractor will:
Review and manage quarterly OS updates, firmware updates and security patches on a monthly basis and install updates as neededand/or on a minimum quarterly basis. Critical patches shall be installed within 30 days of notice.

6. PCI Support

Contractor will:

Provide assistance with credit card data key encryption changes and OS password changes. Provide that all passwords will meet minimum complexity requirements.
Provide visual inspection to ensure all locks are in working order, no credit card skimmers exist, and for signs of tampering of equipment.
Inspect of each workstation to ensure no unnecessary or unwanted applications are installed and/or running.
Provide monthly PCI DSS checklist 12.11 to attest service provider (SKIDATA) is performing their services for the John Wayne Airport PARCS system stated in the Statement of Work related to PCI Compliance.

7. Operations
Contractor will:
Provide remote assistance with but not limited to rate changes, validation setup, password lockout, article and user group setup, software setup changes and ad hoc reporting.

8. Wear Parts
Contractor will:
Provide shear bolts, UPS batteries and locking assemblies in need of repair or replacement as a result of normal wear and tear.
Provide thermal print heads when Certified SKIDATA tickets are used.

9. Response
Contractor will:
Provide expedited response to a service calls by the County or the County's Parking Operator.
Priority Definition: There are four priority levels for service requests ranging from Priority-1 (the highest priority) to Priority-4 (the lowest priority). Each priority level will have a required response time, as further defined in table below.

10. Service Level Priority Definitions

Priority	Scope	Examples
1 Emergency	An entire critical sub-system is down or an entire parking structure is inoperable. **Critical sub-systems include application servers (SKIDATA, Parking Guidance, Anti-Virus, Domain), data servers (SKIDATA or PARCS), Credit Card System, LPI System, , Card Access System, Intercom System (entire system or two or more units down in the GTC)*	• Any parking facility cannot exit any cars • The Credit Processing System is down • An entire entry or exit plaza within a structure is down
2 Urgent	An important sub-system is down or a major aspect of a parking structure is not functional. **Important sub-systems include PARCS Workstations, Entry Lanes (two or more in a single structure), Pay of Foot, Exit Lanes (two or more in a single structure), Parking Space Count System as requested by County*	• A manned cashier booth is down • Two or more express lanes are down simultaneously within a single parking structure

3 Normal	Normal: Normal, daily break/fix activity.	• LPI handhelds not working or not functional in one structure • Coder not functional • POF lock broken • One of the master handsets in the Command Center is not functional • An electronic sign at an entry or exit lane is not functional or parking spot counts are reporting incorrect as deemed by parking operator
4 Scheduled or Planned	Scheduled Maintenance or Priority 1 – 3 as requested by County.	• Routine Scheduled Maintenance activity • If we have permission for delay on Priority 1–3, the authorized Customer contact name must be logged

11. Airport Operational hours

Airport Operational hours are from 0500-0000 hours PST 365 days of the year.

12. Service Level Response Time During Airport Operational Hours

Priority	Remote Response	On-Site Response
1	1 hours	2 hours of service call
2	2 hours	2 hours of service call
3(1)	4 hours	8 hours of service call
4(1)	As Scheduled	As Scheduled

13. Airport after hours

Airport after hours is defined as 0001 - 0459 hours PST 365 days of the year.

14. Service Level Response Time During Airport After Hours

Priority	Remote Response	On-Site Response
1	1 hour	2 hours of service call
2	2 hours	2 hours of service call or 6 am, whichever is last
3(1)	10:00 AM the Next business day	12:00 Noon the Next business day

4(1)	As Scheduled	As Scheduled

(1) Priority 3 and Priority 4 service requests will be addressed Monday through Friday during normal SKIDATA business hours, excluding holidays.

15. Response and Report Time

Contractor will:

Comply with response times will be according to the Service Level Response Times tables in this contract.

Notify the County Project Manager and support staff via email sent to JWAAstea@ocair.com when a service request can/cannot be resolved and completed during the first visit.

Notify the JWA Maintenance Service Desk immediately via email sent to JWAAstea@ocair.com.of any unresolved issue and expected time/date when request is anticipated to be resolved.
Failure to do so may result in assessment of penalties in accordance with Attachment F Schedule of Deductions.

16. Repair Time

Contractor will:

Provide a correction or workaround for Priority one (1) and two (2) errors within twenty-four (24) hours from JWA's first reporting to SKIDATA as defined by the date/time service request is submitted through Astea online portal, provided a call is also placed to the Help Desk line immediately following the online submission.

Provide a correction or workaround for Priority three (3) errors within seventy-two (72) hours from JWA's first reporting to SKIDATA, as defined by the date/time service request is submitted through Astea online portal and/or a call is also placed to the Help Desk line, whichever is earlier.
Provide a correction or workaround for Priority four (4) errors within seventy-two (72) hours of scheduled service by SKIDATA, as defined by the date/time provided within the notification to JWA that a service call has been scheduled.

Failure to do so may result in assessment of penalties in accordance with Attachment F Schedule of Deductions.

17. Total Service

Contractor will:

Respond to unscheduled service calls for remedial maintenance (as a result of normal wear and tear) performed in response to Customer's request on a twenty-four (24) hours per day basis throughout the year, including holidays.

18. Planned Downtime

Contractor will:

Provide planned SKIDATA downtime for Systems maintenance, for a maximum of eight (8) hours four (4) times per calendar year for the duration of the contract.
Any additional planned downtimes will be billed at established rates for Non-Covered Services.

19. Obsolete and Unsupported Software or Hardware

Contractor will:

Notify customer (John Wayne Airport) of any hardware or software, currently in use that will go unsupported within nine (9) months of obsolescence.
Ensure that this notice is sent to the County's project manager and JWA Purchasing department with a report that details the support needed to maintain operational status and a proposal to maintain operational status beyond obsolescence.

20. Service Request Reporting

Contractor will:
Produce monthly, or on demand, reports and data extracts on the service request data.
Provide a mechanism whereby JWA is able to run and print these reports independently if so desired by the County if available.

1. Report Formats

Reports will be provided in Excel, Word, or PDF format as requested by JWA if available by SKIDATA's accounting system.

   a. Data extracts will be provided in either Excel or comma separated value (CSV) formats as requested by JWA.

   b. Reports will be provided in electronic format only.

2. Report Content

   a. Service Level summary: Summarizes all service requests made within the reporting period including the number of calls received, the average response time, average time to arrive on-site, and average repair times for each service level. If run for longer than a single day, the report must include summaries for each day, each week, and each month within the reporting interval. For example, a report run from January 1 through February 28 will show the numbers for each day, as well as the roll-up numbers for each week, for January, and for February.

   b. Service Level Compliance: A single-page summary of the service level compliance for the reported period. It will include the total number of service requests, the number of requests that are out of compliance, and details for each service request that is out of compliance for each priority level. The service request details can use as many additional pages as needed.

   c. Service request details: Detailed information about any individual service request. The report must be runnable on a single request, a list of requests, a range of requests, or all requests within a user-defined time period. This report is only available in a PDF Work Order format.

   d. Service request summary: Summary information about an individual service request. The report must be runnable on a single request, a list of requests, a range of requests, or all requests within a user-defined time period. This report is only available in a PDF Work Order format.

   e. Custom reports: JWA may request custom reports be developed on service requests and service levels at an additional charge. Provided that the requested information is available and it is feasible to create the report, SKIDATA will make best efforts to meet the request.

      - JWA will request the custom report in writing and will include a sample of the desired report content and format.
      - SKIDATA will provide a cost proposal for the report development within 10 business days.
      - JWA will review the proposal. If the proposal is accepted, JWA may issue a Purchase Order number to SKIDATA to proceed with development.

3. Data extracts

   a. Labor and material transaction activity on service requests will be provided in data extracts.

b. JWA may request custom data extracts be developed at an additional charge. Provided that the requested information is available and it is feasible to create the extract, SKIDATA will make best efforts to meet the request.

- JWA will request the custom data extract in writing and will include a sample of the desired extract content and format.
- SKIDATA will provide a cost proposal for the extract development within 10 business days.
- JWA will review the proposal. If the proposal is accepted, JWA will issue a Purchase Order number to SKIDATA to proceed with development.

4. Report Due Dates

SKIDATA will provide the Service Level Summary and Service Level Compliance reports by the 5th business day of each month for the preceding month. The reports must be submitted with the monthly maintenance invoice.

II. Contractor Responsibilities

Before leaving the JWA location and/or closing any service request, SKIDATA will obtain confirmation from the parking operator that a reported problem has been resolved to the operator's satisfaction by obtaining an authorized representative's signature on an electronic Work Order, which is then submitted via email at JWAAstea@ocair.com as formal notification of resolution and/or necessary work-arounds. The name of the person approving the service request closure must be noted in the service request so that it will appear in the service request reports.

Must follow all JWA procedures for processing service requests and interacting with the JWA Maintenance Service Desk.
Must follow all airport rules and regulations at all times.
Must properly dispose of all trash and debris generated by their activities at the end of each workday.

Provide technicians who have a minimum of one (1) year experience on the component on which they are working and who are factory certified as fully qualified to be engaged in the activity on which they are working. Technicians who do not meet these qualifications will not be permitted to work on any JWA systems, software, or equipment.

A. Contractor Vehicles

Must have the business name clearly shown and affixed to the exterior of the vehicle.
Must be locked and a business card with contact information for the driver must be placed on the dashboard of the vehicle in a manner that it is clearly visible and readable from outside the vehicle.
County provided parking access cards are not to be used outside the scope of this contract.

B. Network (Contractor)

Contractor shall cooperate with JWA IT to resolve network failures or problems.
Provide labor to resolve issues associated with planned and unplanned network outages.
For planned outages see Section 18, Planned Downtime.

C. Change Management

Contractor will follow JWA change control process as detailed in this section and ATTACHMENT C COUNTY OF ORANGE INFORMATION TECHNOLOGY SECURITY STANDARDS. All changes will be correctly documented and must be fully approved by both parties prior to implementation.

A JWA IT Change Request Form (County of Orange Change Request Clause does not apply) will be completed by Contractor's staff and submitted for approval to JWA. Normal Change Requests require a minimum three (3) days in advance. If it is less than three (3) days, then an Emergency Change Request is required and indicated on the JWA IT Change Request Form. Reference Attachment E – John Wayne Airport – IT Change Request Form.

D. Rate Forecasting Model

The Rate Forecasting Model is a software feature of the PARCS. It allows JWA to estimate future revenues based on historical data, projected growth, and theoretical future rates.

1. Database Updates

Contractor will provide updates to the Rate Forecasting Model database

2. Changes to the Rate Forecasting Model Application

Contractor will provide labor for County requested changes to the application

E. Payment Card Industry (PCI) PA-DSS Validation Provisions

See Responsibility Matrix for details. Reference Attachment I.

1. PCI Standards

The JWA PARCS system as a whole has been certified, by Tevora as an independent QSA, to be PCI DSS v3.2.1 compliant as of October 2022.
The payment applications are currently certified to be PCI PA DSS 3.2 compliant.
Contractor will maintain the JWA PARCS system to meet continued compliance.

2. Activities Required to Support PA-DSS Validated Payment Applications for PARCS.

Contractor will:

a. Provide labor to maintain SKIDATA and Payment Express and other installed software per the Secure Implementation Guide based on the PA DSS v3.2 requirements.

b. Provide labor to keep anti-virus software and Microsoft products current.

c. Provide labor to install updates to the two validated payment applications and associated fees due to PCI standards PCI DSS current active version are included in the monthly maintenance fee.

d. Provide labor to make changes to IP addresses, VLANs, as a result of changes to PCI standards or versions are not included in the monthly maintenance fee.

e. Provide labor to remove existing equipment and install new equipment and any equipment costs associated with changes to PCI standards or versions are not included in the monthly maintenance fees.

For any events listed above that are not covered by the monthly maintenance fee, SKIDATA will provide a cost proposal to JWA using the rates in Attachment B associated with this Scope of Work. If the proposal is accepted, JWA will issue a Task Order for SKIDATA to proceed with the work.

F. Activities Required to Demonstrate PCI Compliance

John Wayne Airport ("JWA") is required to establish Payment Card Industry Data Security Standard ("PCI DSS") compliance and that utilize the services of SKIDATA Control Systems ("SKIDATA") for Parking and Revenue Control System ("PARCS") maintenance.
JWA's PCI DSS assessment is required to cover SKIDATA's maintenance service that permits SKIDATA to impact the security of JWA's cardholder data environment.

As a result, SKIDATA will assist in JWA's PCI DSS compliance validation process by providing the following in the format mandated by current PCI DSS requirements and timing as directed by JWA's project manager(s):

1. A high-level dataflow diagram showing how SKIDATA's maintenance services interface with JWA's environment.
2. Network diagrams
3. Evidence of system-patching methodology and, if applicable secure coding methodology.
4. Results of SKIDATA's internal and external vulnerability scans, if available.
5. Security policies and operational procedures.
6. Access to systems, facilities, and appropriate personnel for on-site reviews, interviews, physical walk-throughs.
7. Review and explanation of SKIDATA's policies, procedures, process documentation, configuration standards, training records, incident response plans that evidence SKIDATA's satisfaction of applicable PCI DSS requirements and/or that SKIDATA adheres to JWA's policy.
8. Review of evidence such as configurations, screen shots, and process reviews, to assist in validating all applicable PCI DSS requirements are being met for the in-scope components maintained by SKIDATA.
9. Clarity regarding portions of JWA's PARCS merchant environment subject to maintenance by SKIDATA that is in scope for JWA's PCI DSS assessment.
10. Retention of evidence collected due to non-compliance with PCI DSS.
11. Forty (40) hours of SKIDATA's labor time associated with annually demonstrating JWA's site compliance with the PCI DSS current active version is included. Labor exceeding forty (40) hours labor annually will be billed to the County per rates specified in Attachment B
    i. This includes time preparing for and participating in meetings and conference calls, and preparing requested documentation, including but not limited to screenshots, flow charts, forms, narratives and diagrams.
    ii. This also includes time preparing for and participating in activity associated with JWA's PCI site compliance including but not limited to scans and network penetration testing.
    iii. Failure to do so may result in assessment of penalties in accordance with Attachment F Schedule of Deductions.

Upon contractor notification of five (5) business days of PCI Audit schedule, provide the requested PCI documentation within two (2) business days. Failure to do so may result in assessment of penalties in accordance with Attachment F Schedule of Deductions.

12. Activities Required to Support JWA's Site Compliance

If the required activities are made necessary by an error or omission in SKIDATA's maintenance of the system, those activities will be performed at no additional cost to the County.
If the required activities are made necessary by changing PCI DSS standards or the County's changing requirements, SKIDATA's labor time associated with supporting JWA's site compliance are included. This includes time to research, respond to, or remediate gaps identified by JWA and/or its Qualified Security Assessor (QSA) to support JWA's site compliance.

G. Invoicing

Contractor will:
Provide an invoice to the County at the end of each month.

H. Invoicing (Parking Operator)

The contract between the County and the parking operator obligates the parking operator to accept responsibility for certain types of damage and charges resulting from failure to operate and maintain the systems correctly.

When directed by the County, Contractor will submit separate invoices for those fees and charges directly to the parking operator.

Notify the County in the event the parking operator fails to promptly pay invoice(s).

I. Non-Covered Services

Non-covered services requested by County to be performed will be provided at Contractor's rates as set forth in the ATTACHMENT B CONTRACTOR'S PRICING as "Rate Schedule for Non-Covered Services" and "Non-covered parts".

J. Systems Upgrade Project

The following systems, equipment, software, or hardware changes are necessary to extend the usable life of the systems and must be completed within 8 months from execution of the order. All work must be coordinated with JWA prior to start. Reference Attachment E Proposal.

1. **JWA – 2023 SAAS Upgrade**
   a. Upgrade existing PARCS system and lanes to software version 15 using SKIDATA's Software as a Solution (SaaS) subscription.
   b. SKIDATA's SaaS annual subscription unlocks most software modules, provides quarterly software updates and software upgrades, as released, and sweb services including Control Basic,

III. County Responsibilities

A. Incidents / Faults
The County will be provide the following information.
1. Name and telephone number of individual placing Service request
2. Description of issue
3. Troubleshooting steps already performed
4. Location of issue
5. Priority of the issue as defined in table below
6. Contact name and phone number

B. Parking Operator
The County will communicate with the County's Parking Operator to provide the Contractor with all necessary access to staff, facilities, and systems required to resolve a service request issue.

C. Remote Access
The County will provide to Contractor remote access required to facilitate timely maintenance and repair activities.

D. Network (County)
Cisco Equipment
The County will maintain a hardware and software maintenance on all Cisco network equipment used by PARCS.

E. Network Change Requirements (County)
County will provide Contractor procedure and documentation for JWA change control processes. Reference section II, subsection c. Change Management.

F. Monthly and Quarterly Meetings

1. Monthly Meetings

Operations personnel from JWA and SKIDATA agree to meet each month at a mutually agreed upon date and time and at a mutually agreeable venue (in-person or remote) to review operational matters.

Topics for review include:

- Service request reports for activity the prior month
- Service level performance metrics for the prior month
- Preventative maintenance activities performed by the parking operator the prior month
- Preventative maintenance activities performed by SKIDATA for lane equipment and IT equipment (reviewed once per quarter)
- Communication concerns or issues by either party
- Training needs by JWA or the parking operator
- Other topics as needed.

2. Quarterly Meetings

Senior management personnel from JWA and SKIDATA agree to meet quarterly at a mutually agreed upon date and time to review:

- Overall compliance of the parties to this agreement
- Status of the relationship between the parties
- Contract terms that may need to be amended and that are mutually agreed upon
- Trends in technology and/or the parking industry that may affect or be of interest to either party
- Upcoming significant projects that may affect both parties (e.g., transition to SKIDATA Releases, planned County upgrades or changes to the network, planned County outages)
- Proposals for installation of new equipment
- Other topics as needed.

IV. Additional Work:

A. Upon County request, Contractor shall submit supplemental proposals for Additional Work not called for under the Scope of Work of this Contract. Contractor must obtain County Project Manager's written approval prior to commencing any additional work.
B. County reserves the right to obtain supplemental proposals from, and use, alternate sources for completion of the additional work and to utilize the data provided under this Contract to obtain necessary services.
C. If County authorizes work by an alternate source, Contractor may be relieved of responsibilities pertaining to the equipment affected by the project while work is being performed and during the subsequent warranty period.
D. Contractor shall continue to provide services to all areas not affected by work provided by alternate sources.

Upon completion of any additional work, whether by Contractor or an alternative source, County's Project Manager or designee and Contractor will inspect the finished product at no additional cost to County. Upon mutual acceptance of the additional work, Contractor shall again be responsible for all services originally covered under this Contract and the work performed under this section.

ATTACHMENT B
CONTRACTOR'S PRICING

This is a firm fixed rate contract between County and Contractor, as set forth in Attachment "A" Scope of Work.

A. Compensation

The Contractor agrees to accept the specified compensation as set forth in this Contract as full payment for performing all services and furnishing all personnel 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.

Contract not to exceed $2,257,644

B. Fees and Charges

Fee and Charges			
Description	**Year 1**	**Year 2**	**Year 3**
Covered Services	$ 255,041	$ 262,693	$ 270,573
Covered Parts	$ 341,986	$ 352,245	$ 362,813
LPI	$ 4,098	$ 4,221	$ 4,347
PM Services Total	**$ 601,125**	**$ 619,159**	**$ 637,733**
SaaS Upgrade Project Setup	$ 9,027		
SaaS Upgrade Project Subscription	$ 55,200	$ 55,200	$ 55,200
Additional Work	$ 75,000	$ 75,000	$ 75,000
Grand Total	**$ 740,352**	**$ 749,359**	**$ 767,933**

1. Covered Services, Covered Parts and LPI
   a. Reference Fee and Charges Table
   b. County shall pay the following fees monthly in accordance with the Payment Terms – Payment in Advance, herein.

2. SaaS Upgrade Project
   a. Reference Exhibit B SaaS Upgrade Project
   b. County shall pay the following fees in accordance with the Payment Terms – Payment in Arrears, herein.

3. Additional Work - Non-Covered Services

Non-Covered Services			
Labor for Service Technician			
Time of Service	**Minimum Time Period**	**Hourly Rate for Minimum Period**	**Hourly Rate for After Minimum Period**
Regular Hours (8:00 am – 5:00 pm)	One-Half Hour	$97.50	$195.00

After Hours (5:01 pm – 7:59 am)	Half Hour	$195.00	$390.00
Holidays	Half Hour	$219.38	$438.75

a. Standard Rate Schedule - Regular Service (Monday – Friday, 8am – 5pm)

b. Standard rates are billed in 30-minute increments with minimum periods defined in the table above. Time exceeding any 30-minute increment is rounded up to the next increment. These rates are applicable during normal SKIDATA business hours.

c. Contractor's holidays defined as:
New Year's Day, Martin Luther King Day, President's Day, Memorial Day, Independence Day, Labor Day, Thanksgiving Day, Day after Thanksgiving, Christmas Eve, Christmas Day

County shall pay the following fees accordance with the Payment Terms – Payment in Arrears, herein

4. Additional Work - Non-Covered Parts
   a. Reference Attachment G Out-of-Scope Non-Covered Parts Pricing 2023
   b. Rate Schedule Material Not Included In Attachment G
      - Cost + 15% or a minimum handling fee of thirty dollars ($30.00). Tax and shipping not included.
      - For custom prints on tickets or keycards, please contact contractor.
      - 15% discount on parts orders
      - All prices are excluding. transport and shipping costs.
   c. County shall pay the following fees monthly in accordance with the Payment Terms – Payment in Arrears, herein.

C. Renewal Years Fees and Charges

Renewal Years Fees and Charges		
Description	**Year 4**	**Year 5**
Covered Services	$ 278,691	$ 287,051
Covered Parts	$ 362,813	$ 373,697
LPI	$ 4,478	$ 4,612
PM Services Total	**$ 645,981**	**$ 665,360**
SaaS Upgrade Project Setup		
SaaS Upgrade Project Subscription	$ 55,200	$ 55,200
Additional Work	$ 75,000	$ 75,000
Grand Total	**$ 776,181**	**$ 795,560**

D. Final Payment

Final payment shall be issued based on the completion of the work as described in this Contract and County Project Manager accepts the all work and JWA issued badges are returned to Badging Office.

E. Payment Terms – Payment in Arrears

Invoices are to be submitted in arrears to the user agency/department to the ship-to address, unless otherwise directed in this Contract. Contractor shall reference Contract number on invoice. Payment will be net 30 days after receipt of an invoice in a format acceptable to 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 with County providing written notice of any unacceptable invoices within 10 days of receipt. Contractor, upon receiving notice of the unacceptable invoice, shall provide an acceptable invoice within 10 days. In the event an invoice is disputed, the parties shall act in good faith to resolve the dispute within 30 days of written notice of a dispute.

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.

F. Payment Terms – Payment in Advance

Invoices are payable 30 days in advance, unless otherwise directed in this Contract. Invoices are to be submitted to the user agency/department to the ship-to address, unless otherwise directed in this Contract. Contractor shall reference Contract number on invoice. Payment will be net 30 days after receipt of an invoice in a format acceptable to 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 rest 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.

G. 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.

H. 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:

1. Contractor's name and address
2. Contractor's remittance address, if different from 1 above
3. Name of County Agency/Department
4. Delivery/service address
5. Master Agreement (MA) or Purchase Order (PO) number
6. Date of order
7. Product/service description, quantity, and prices
8. Sales tax, if applicable

9. Freight/delivery charges, if applicable
10. Total

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

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

Email to:

AccountsPayable@ocair.com

ATTACHMENT C
COUNTY OF ORANGE INFORMATION TECHNOLOGY SECURITY STANDARDS

(attached separately)

ATTACHMENT D
STAFFING PLAN

Contractor shall

A. Supply a list of contractor personnel in conjunction with this contract

B. Submit any changes to be approved by County or designee

The substitution or addition of contractor personnel in any given category or classification shall be allowed only with prior written approval of County Contract coordinator or designee.

#	Name	Title/ Classification	Area/Description of responsibility
1	Vincent Ramirez	System Engineer	IT & software maintenance
2	Stephany Salas	Service Advisor	Customer Support
3	Abraham Ponce	Manager Customer Support	Customer support
4	Carlos Serrano	Field Service Manager	Field Service delivery
5	Daniel Soria	Manager Technical Support	Technical Support
6	Mary Beth McNair	Key Account manager	Sales/KAM
7	Chris McKenty	Key Account manager	Exec/KAM
8	Ramon Embrador Donne Ngueneba	Field service technicians	Field service
9	TDB	Project manager	Project/contract mngt
10	TDB	System Engineer	IT & software maintenance

ATTACHMENT E
JOHN WAYNE AIRPORT – IT CHANGE REQUEST FORM

(attached separately)

ATTACHMENT F
SCHEDULE OF DEDUCTIONS

In the event that Contractor fails to comply with these service level agreements may result in penalties in accordance with the following Attachment F Schedule of Deductions. County project manager reserves the right to deduct fees from Contractor's monthly invoice.

Schedule of Deduction	
System Service Level Agreements	**Penalties**
Response and/or Repair – Priority 1	$2,000.00 per occurrence per day
Response and/or Repair – Priority 2	$1,000.00 per occurrence per day
Response and/or Repair – Priority 3	$500.00 per occurrence per day
Response and/or Repair – Priority 4	$250.00 per occurrence per day
Miscellaneous Items	
Response and/or Report Requirements	$100.00 per occurrence per day
PCI audit reporting and support	
PCI documentation beyond the allowed two (2) business days and/or PCI Compliance requests	$500.00 per occurrence per day

g

ATTACHMENT G
OUT-OF-SCOPE NON-COVERED PARTS PRICING

Item number	Description	Price
	Column 2000	
10047-001	Ticket Bin	$293.00
PFLT-UNLIMITED	Press for Lost Ticket	$4.83
PFRT-UNLIMITED	Press for Return Ticket	$1.23
PFT-UNLIMITED	Press for Ticket	$1.23
	Power.Gate	
546200468	Ticketbox, Power.Gate	$439.26
	Coder 460	
546010007	Thermal Printhead Coder 460	$1,607.02
546010007R	Thermal Printhead Coder 460 (refurbished)	$1,411.00
546010049-1	Prism Set Coder – Prism T	$4.33
	Barrier.Gate	
546521000	AC-Barrier.Gate-BOOM 3.0	$625.00
546521001	Boom Profile, Barrier.Gate – Yellow, 3m	$1,100.85
546521026	Barrier.Gate RGB LED 9.84 (stocked)	$1,373.75
546521080	Arm, Barrier.GateFOLDING, ADA spare part	$1,373.75
546521135	Sheer Bolt, Skidata Barrier.Gate	$12.50
946521000	Arm, Barrier.Gate Non Illum 9.84	$625.00
946521002	Barrier.Gate Non Illum 11.81	$625.00
946521004	Arm, Barrier.Gate Non Illum 14.75	$625.00
946521012	Arm, Barrier.Gate Yellow LED 9.84	$1,248.75
946521014	Arm, Barrier.Gate Yellow LED 11.81	$1,373.75
946521026	Barrier.Gate RGB LED 9.84	$1,373.75
946521032	Arm, Barrier.Gate RGB LED DEMO 3.28	$1,033.69

946521036	Barrier.Gate FOLDING RGB LED ADA	$3,373.75
946521080	Arm, Barrier.Gate FOLDING, ADA-compliant	$1,373.75
946521081	Arm, Barrier.Gate FOLDING, ADA- Extend	$1,373.75
546521137	Barrier.Gate arm cap transparent	$131.32
	Thermo Validator	
942400200	Thermal Validator	$1,396.20
9454006xx	Printhead for Val Stamp # Nrxx	$247.50
T1112-P5P-ND-1	Power Supply, Thermal Validator	$34.83
	Cleaning Material	
SENTRY460CLEANKIT	Sentry's 460 Cleaning Kit	$62.88
DISKO-1602-1	Cleaning Pads, DISKO Co460	$2.50
DISKO-1642-1	Cleaning Swab, DISKO Flexible	$1.15
DISKO-1668-100ML	Clean Fluid, DISKO Co460 100ml	$30.00
CPZ4108	Card, Cleaning Initialization	$5.73
CPZ4400_0020-1	FELT Cleaning Card-3 Strips	$3.02
	Consumable Products	
METRO-RR	METRO Approved Receipt Rolls, Blank	$87.50
NAGELS-TK450	NAGELS Thermal Tickets 450	$152.50
NAGELS-TK460	NAGELS Thermal Tickets 460	$175.00
1326LMSMV	Card, HID Proxcard II Std	$5.25
1346LNSMN	Keyfob, ProxKey® II RF Prog.	$11.00
CP001259	SkiData Thermolabel	$0.25
CP019215	SkiData Blank Keycard, R20	$9.50
CPZ2120	SkiData Receipt Rolls Power & Lite Gate	$30.00
AH-CSAWID00	Shell Card, AWID Prox Clam Shell	$3.95
1346LNSMN	HID Prox Key III 1346 Key Fob	$11.00
S1255	nly Tags	$58.75

S1938	Tag Holder for MeM Tag (S1240)	$6.25
S1951/00	TagMaster WinFix, (S1255)	$5.25
1386LGGMN	HID Isoprox II Card	$8.75
945010428	Spare Keys for Column 2000, Power.Gate and Barrier.Gate	$61.59
KEY-010	Key for MS Cashdrawer 102	$7.00

ATTACHMENT H
SKIDATA RESPONSIBILITY MATRIX
(attached separately)

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 shall maintain an inventory of its services. This listing shall be used by the department 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 policy.

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 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 shall maintain an inventory of all department 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 shall adopt a standard naming convention for devices (naming convention to be utilized as devices are serviced or purchased) that, at a minimum, includes the following:

- Department (see Appendix A for an example Department Listing)
- Facility (see Appendix B for an example Facility Listing)
- Device Type (see Appendix C for an example Device Type Listing)

1.2.3.4 Each department 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 shall maintain an inventory of its facilities. This listing shall be used by the department to assist with its risk management analysis.

1.2.4.2 Departments shall identify the facilities used by its critical services.

1.2.5 Access Controls

Refer to *User Provisioning Policy* for additional guidance.

1.2.5.1 Departments 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 are to be assigned a unique user ID to access the network.

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 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 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 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' 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 policy, 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. See Section on Encryption.

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 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. If the device ("i" device or smartphone, only) complies with the mobile device management security standards (see section 9.2.3 Mobile Computing Devices), this is not applicable.

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 Microsoft Office 365 environment, OC Expediter, and VTI timesheet applications, to name a few. 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 device 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 (see Section 9.2.4 Mobile Computing Devices for additional guidance on mobile devices) and personally owned devices used for work (see Section 9.2.5 Personally Owned Devices for additional guidance on personally owned devices).

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 upper case letter
- Passwords will contain a minimum of one lower case letter
- Passwords will contain a minimum of one number: 1- 0
- Passwords will contain a minimum of one symbol: !,@,#,$,%,^,&,*,(,)
- 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

2.2.7.3 Passwords shall have a minimum length of 8 characters.

2.2.7.4 Passwords shall not be reused for twelve iterations.

2.2.7.5 Departments 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 in accordance with Section 12: Incident 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 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 (refer to Section 9.2.4 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, customers or vendors 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 (e.g., DISO) using the 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 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 9.2.8.

2.2.11 Remote Access

2.2.11.1 Departments 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 members 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 OCIT Enterprise Privacy and Cybersecurity. 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 infrastructures 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 infrastructures shall be reviewed and approved by both the department DISO and OCIT Enterprise Privacy and Cybersecurity. This approval shall be received prior to the start of such implementation. The approval shall be developed as a memorandum of understanding (MOU).

2.2.11.11 Remote access privileges to County IT resources shall not be given to contractors, customers or vendors 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 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 OCIT Enterprise Privacy and Cybersecurity 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, vendors 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 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 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 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 white listing and black listing 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 shall implement host-based Data Loss Prevention (DLP) to reduce the risk of data breach related to sensitive information.

2.2.16.2 Departments shall deploy encryption software on mobile devices containing sensitive. See Section 9.2.19 Encryption for additional guidance.

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 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 (as defined by County policy) 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:

- Determination of the level of cryptographic controls
- Key management/distribution steps and responsibilities

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

2.2.19 System Acquisition and Development

2.2.19.1 Departments 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).

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 policy provided in Section 7: Access Control.

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 policy.

2.2.19.5 In situations where data needs to be isolated because there would be a conflict of interest (e.g., DA and OCPD data cannot be shared), 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 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 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 9.2.8: 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 (once policy is effective) for systems containing sensitive information.

> Contractor shall report to the County within 24 hours as defined in this contract when Contractor becomes aware of any suspected data breach of Contractor's or Sub-Contractor's systems involving County's data.

2.2.20.2 Departments shall review all procurements and renewals for software and equipment (hosted/managed by the vendor) that transmits, stores, or processes sensitive information to ensure that vendors and contractors are aware of and are in compliance with County's cybersecurity policies. Departments shall obtain documentation supporting the business partners, contractors, consultants, or vendors compliance with County's cybersecurity policies such as:

- SOC 1 Type 2
- SOC 2 Type 2
- Security Certifications (ISO, PCI, etc.)
- 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 OCIT (e.g., security architecture, security appliances, County firewall, Website listings, application listings, email gateway, administrative accounts) shall be reviewed by OCIT Enterprise Privacy and Cybersecurity 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 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 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 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 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 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 Orange 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 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 DISO shall act as the liaison between applicable parties during a cybersecurity incident. The DISO shall be the department's primary point of contact for all IT security issues.

5.2.9 A directory or phone tree shall be created listing all department cybersecurity incident liaison contact information.

5.2.10 Departments 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 shall develop and document procedures for reporting cybersecurity incidents. For example, all employees, contractors, vendors 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 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 shall report cybersecurity incidents to the Central IT Service Desk in accordance with the County's Cyber Incident Reporting Policy.

5.2.17 Confirmed cybersecurity incidents that meet the criteria defined in the Significant Incident/Claim Reporting Protocol shall be reported by the County's Chief Information Security Officer to the Chief Information Officer (CIO), County Executive Officer (CEO), and the Board of Supervisors within 24 hours of determination that a cybersecurity incident has occurred.

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 executed and reviewed.

6.2 SERVICE CONTINUITY MANAGEMENT POLICY STATEMENTS

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

6.2.2 Each department 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 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 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 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 shall develop, periodically update, and regularly test business continuity and disaster recovery plans in accordance with the County's Business Continuity Management Policy.

6.2.11 Departments shall review and update their Risk Assessments (RAs) and Business Impact Analyses (BIAs) as necessary, determined by department management (annually is recommended). As detailed in Section 14: Risk Assessment and Treatment, 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 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. Plans shall be prepared in accordance with the standards established by the County's Business Continuity Management Policy.

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

John Wayne Airport – IT Change Request

(Please print legibly)

Priority	**Change Category** *(check all that apply)*	**Control Item** *(check all that apply)*
☐ Emergency ☐ Non-Emergency **Frequency** ☐ One-Time Change ☐ Recurring Change Ending date: *(leave blank if not applicable)* ***Click or tap to enter a date.***	☐ Break fix ☐ Code change ☐ Enhancement ☐ Patch ☐ Other (specify) _____	☐ Server ☐ Network ☐ Software ☐ Other (specify) _____

Change Request #:

Requestor / Engineer's Name:		
Originator:		
Proposed Production Change Date:		
Target Systems/Equipment/Applications:		
Estimated Change Duration:	Start: m/dd/yy hh:mm End : mm/dd/yy hh:mm	
Back-Out Time (drop dead):	Time: mm/dd/yy hh:mm	

Description of Requested Production Change (if an emergency please explain why)

High Level Reasons for Production Change

Work Plan for System Change (please describe step by step what work is being done)

Key Assumptions (define what you anticipate will happen during the CR)

Acceptance Testing (define the testing that will determine success for this CR)
Type acceptance testing steps here: 1. 2.

Back-Out Plan (If the change fails, how will operations be restored?)

Impact Assessment (define in detail the impact to the Users and the Systems)

RESOURCE and SUPPORT CHECKLIST

Yes	No	NA	Checklist Item
			IT and User notification draft prepared
			User notification required?
			Admin support documents completed
			User support or instruction documents sent to the Help Desk Lead

			Impacted staff or users training completed
			Procedures testing complete
			Restore testing complete
			System Documentation Updated

Change Notification Draft

IMPACTED CUSTOMERS: (Who)
ACTIVITY REQUIRED: (What)
ACTIVITY TIME LINE: (When)
USER IMPACTS: (What should those impacted expect to happen and who can they contact) :
SYSTEM IMPACTED: (What system) :
EXECUTIVE SPONSOR: (Name of Business Owner) :

Additional Notes

Inventory Updates / Documentation Updates
(this section details the updates to the equipment inventory required reflecting changes effected by this change request.)

Closure Result and Notes
(indicate final disposition of change and provide proof via detailed notes or attach screenshots)

Change Result: Successful ☐ Failed ☐

Approval to implement:_____ Date:_____
(Name)

_____
(Signature)

Completed by: _____ Date:_____
(Name)

_____
(Signature)