AMENDMENT TWO TO CONTRACT

BETWEEN

COUNTY OF ORANGE

AND

ARBOR E&T, LLC DBA EQUUS WORKFORCE SOLUTIONS

FOR THE PROVISION OF INTEGRATED JOB SERVICES

THIS AMENDMENT TWO**,** made and entered into upon execution of all necessary signatures, is to that certain CONTRACT Number WDM0922 between the parties hereto, hereinafter referred to as the "Contract" and is by and between the COUNTY OF ORANGE, hereinafter referred to as "COUNTY," and ARBOR E&T, LLC DBA EQUUS WORKFORCE SOLUTIONS, hereinafter referred to as "CONTRACTOR." COUNTY and CONTRACTOR may be referred to individually as "Party" and collectively as "the Parties."

W I T N E S S E T H

WHEREAS, on July 1, 2022, COUNTY and CONTRACTOR entered into a Contract for the provision of Integrated Job Services, for the term of July 1, 2022, through June 30, 2025;

WHEREAS, AMENDMENT ONE was issued to amend Subparagraphs 19.4, 21.3.1, and Paragraph 32 of the Contract; amend Subparagraph 4.2 of Attachment A of the Contract; replace Attachment B in its entirety; replace Attachment D of the Contract in its entirety; and add Attachment E to the Contract;

WHEREAS, COUNTY desires to renew the Contract for an additional two (2) years from July 1, 2025, to June 30, 2027; amend Paragraphs 1, 5, 7, 14, 16, 32, and 43, and Subparagraphs 10.4.3, 19.4, 21.1, and 21.2 of the Contract; add Subparagraph 35.4 to the Contract; amend Paragraphs 3, 10, and 12, and Subparagraphs 5.8, 5.14.1, 6.3.3, and 9.2 of Attachment A of the Contract; add Subparagraph 6.3.8 to Attachment A of the contract; and replace Attachments D and E in its entirety; and add Attachment F to the Contract; and

WHEREAS, CONTRACTOR agrees to such extension and to continue to provide such services under the terms and conditions set forth in this Contract;

ACCORDINGLY, THE PARTIES AGREED AS FOLLOWS:

1. Paragraph 1 of the Contract is hereby amended to read as follows:

1. TERM

The term of this Contract shall commence on July 1, 2022, and terminate on June 30, 2027, unless earlier terminated pursuant to the provisions of Paragraph 42 of this Contract; however, CONTRACTOR shall be obligated to perform such duties as would normally extend beyond this term, including, but not limited to, obligations with respect to indemnification, audits, reporting and accounting.

2. Paragraph 5 of the Contract is hereby amended to read as follows:

5. COMPLIANCE WITH LICENSING STANDARDS AND LAWS

5.1   CONTRACTOR warrants that it and its personnel, described in Paragraph 27 of this Contract, who are subject to individual registration and/or licensing requirements, have all necessary licenses and permits required by the laws of the United States, State of California (hereinafter referred to as "State"), County of Orange, and all other appropriate governmental agencies to perform the services described in this Contract, and agrees to maintain, and require its personnel to maintain, these licenses and permits in effect for the duration of this Contract. Further, CONTRACTOR warrants that its employees shall conduct themselves in compliance with such laws and licensure requirements, including, without limitation, compliance with laws applicable to sexual harassment and ethical behavior.   CONTRACTOR must notify ADMINISTRATOR within one (1) business day of any change in license or permit status (e.g., becoming expired, inactive, etc.).

5.2   CONTRACTOR represents and warrants that services to be provided under this Contract shall fully comply, at CONTRACTOR's expense, with all standards, laws, statutes, restrictions, ordinances, requirements, and regulations (collectively "laws"), including, but not limited to, those issued by COUNTY in its governmental capacity and all other laws applicable to the services at the time services are provided to and accepted by COUNTY. CONTRACTOR acknowledges that COUNTY is relying on CONTRACTOR to ensure such compliance, and pursuant to the requirements of the Insurance and Indemnification section, CONTRACTOR agrees that it shall defend, indemnify and hold COUNTY and COUNTY

Indemnitees harmless from all liability, damages, costs and expenses arising from or related to a violation of such laws.

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

In the performance of this Contract, CONTRACTOR shall comply with all applicable provisions of the California Welfare and Institutions Code (WIC); Title 45 of the Code of Federal Regulations (CFR); implementing regulations under 2 CFR Part 200, Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards; Title 48 CFR Section 31.2; and all applicable laws and regulations of the United States, State of California, County of Orange, and County of Orange Social Services Agency, and all administrative regulations, rules, and policies adopted thereunder, as each and all may now exist or be hereafter amended.

5.3   For federally funded Contracts in the amount of $25,000 or more, CONTRACTOR certifies that its officers and/or principals are not debarred or suspended from federal financial assistance programs and/or activities.

3. Paragraph 7 of the Contract is hereby amended to read as follows:
7. SUBCONTRACTS

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

In the event that CONTRACTOR is authorized by COUNTY to subcontract, this Contract shall take precedence over the terms of the agreement between CONTRACTOR and subcontractor, and any agreement between CONTRACTOR and a subcontractor shall incorporate by reference the terms of this Contract. CONTRACTOR shall remain responsible for the performance of this Contract and indemnification of COUNTY notwithstanding the

COUNTY's consent to CONTRACTOR's request for approval of a subcontractor. Under no circumstances shall COUNTY be required to directly monitor the performance of any subcontractor. All work performed by a subcontractor must be monitored by CONTRACTOR and must meet the approval of the County of Orange pursuant to the terms of this Contract.

7.1.1   Subcontracts of $50,000 or less

7.1.1.1   CONTRACTOR shall develop a standard form Purchase Order, subject to prior written approval of ADMINISTRATOR, to be utilized for the purchase of services by CONTRACTOR when the cumulative total cost of the services to be provided by any organization is anticipated to be fifty thousand dollars ($50,000) or less during the term of this Contract. The basis for costs incurred by any such Purchase Order(s) shall be the actual cost of providing services or the usual and customary charges established by the organization(s) providing the services.

7.1.2   Subcontracts in excess of $50,000

7.1.2.1   CONTRACTOR shall develop and submit for approval to ADMINISTRATOR a system for the procurement of subcontracts with any organization in which the total cumulative cost of services provided by any single organization is anticipated to exceed fifty thousand dollars ($50,000) during the term of this Contract. CONTRACTOR's proposed procurement system shall take into consideration such factors as: degree of price competition; pricing policies and techniques; experience and quality of service; methods of evaluating subcontractor responsibility; relationship of subcontractor to CONTRACTOR; and planning, award, and post-award management of subcontracts, including internal audit procedures and monitoring of subcontractor's performance until completion of services.

7.1.2.2   Upon ADMINISTRATOR's approval of CONTRACTOR's proposed procurement system, CONTRACTOR shall comply with such procurement system in obtaining subcontracts with a total cost in excess of fifty thousand dollars ($50,000) during the term of this Contract. In addition, CONTRACTOR shall obtain ADMINISTRATOR's written consent prior to entering into a subcontract with any organization when the total cumulative cost of services to be provided by that organization is anticipated to exceed fifty thousand dollars ($50,000) during the term of this Contract.

7.1.2.3   CONTRACTOR and its subcontractor(s) shall establish and maintain accurate and complete financial records related to services provided under the terms of this Contract. Such

records may be subject to the satisfaction of ADMINISTRATOR, and to the examination and audit by ADMINISTRATOR or designee, for a period of five (5) years, or until any pending audit is completed.

4. Subparagraph 10.4.3 of the Contract is hereby amended to read as follows:

10.4.3 The following websites provide Civil Rights information, publications and/or forms:

10.4.3.1   https://www.cdss.ca.gov/Portals/9/FMUForms/M-P/PUB470.pdf?ver=2021-05-10-164956-817 (Pub 470 - Your rights Under Adult Protective Services)

10.4.3.2   http://www.cdss.ca.gov/inforesources/Civil-Rights/Your-Rights-Under-California-Welfare-Program (Pub 13 – Your Rights Under California Welfare Programs)

10.4.3.3   http://ssa.ocgov.com/about/services/contact/complaints/comply [Social Services Agency (SSA) Contractor and Vendor Compliance page]

5. Paragraph 14 of the Contract is hereby amended to read as follows:

14. INSURANCE

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

14.2   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.

14.3   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. COUNTY reserves the right to require current audited financial reports from CONTRACTOR. If CONTRACTOR is self-insured, CONTRACTOR will indemnify COUNTY for any and all claims resulting or arising from CONTRACTOR's services in accordance with the indemnity provision stated in this Contract.

14.4   If CONTRACTOR fails to maintain insurance acceptable to COUNTY for the full term of this Contract, COUNTY may terminate this Contract.

14.5   Qualified Insurer

14.5.1   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).

14.5.2   If the insurance carrier does not have an A.M. Best Rating of A-/VIII, the CEO/Office of Risk Management retains the right to approve or reject a carrier after a review of the company's performance and financial ratings.

14.5.3   The policy or policies of insurance maintained by 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
Employer's Liability Insurance	$1,000,000 per accident or disease

Network Security & Privacy Liability	$1,000,000 per claims-made
Sexual Misconduct Liability	$1,000,000 per occurrence

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

14.6   Required Coverage Forms

14.6.1   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.

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

14.7   Required Endorsements

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

14.7.1.1   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.

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

14.7.2   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.

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

14.7.3.1   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.

14.7.3.2   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.

14.8   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.

14.9   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.

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

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

14.10.2   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.

14.10.3   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.

14.11   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).

14.12   Insurance certificates should be forwarded to COUNTY at the address indicated in Paragraph 11 of this Contract.

14.13   If CONTRACTOR fails to provide the insurance certificates and endorsements within seven (7) days of notification by CEO/County Procurement Office or ADMINISTRATOR, award may be made to the next qualified proponent.

14.14 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.

14.15 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.

14.16 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.

6. Paragraph 16 of the Contract is hereby amended to read as follows:

16. <u>CONFLICT OF INTEREST</u>

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

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

conflict of interest, CONTRACTOR must also provide an update to COUNTY upon request by COUNTY.

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

7. Subparagraph 19.4 of the Contract is hereby amended to read as follows:

19.4 Use of COUNTY Computer Equipment

COUNTY intends to permit CONTRACTOR the use of computer equipment provided by ADMINISTRATOR.   Said computer equipment shall be used solely by employees of CONTRACTOR while performing their assigned duties pursuant to this Contract, and shall remain the property of COUNTY. CONTRACTOR shall ensure that each of its employees, volunteers, consultants, or agents that have access to COUNTY facilities and/or data contained in ADMINISTRATOR's Computer Information System completes information security and computer usage training provided by ADMINISTRATOR, and adheres to the provisions in Attachments B, C, D, E, and F, to this Contract, signs and adheres to the provisions in SSA Information Technology Security and Usage Agreement as referenced and included in Attachment B, and adheres to any subsequent contracts required by federal or State laws or regulations.   CONTRACTOR's failure to have all CONTRACTOR employees that have access to COUNTY's facilities and/or data execute the contracts and/or complete the training shall constitute a breach of this Contract.

8. Subparagraph 21.1 of the Contract is hereby amended to read as follows:

21.1 Maximum Contractual Funding Obligation

The maximum funding obligation of COUNTY under this Contract shall not exceed the amount of $19,555,350 or actual allowable costs, whichever is less. The estimated annual amount for each twelve (12) month period is as follows:

21.1.1 $3,911,070 for July 1, 2022 through June 30, 2023;

21.1.2 $3,911,070 for July 1, 2023 through June 30, 2024;

21.1.3 $3,911,070 for July 1, 2024 through June 30, 2025.

21.1.4 $3,911,070 for July 1, 2025 through June 30, 2026; and

21.1.5 $3,911,070 for July 1, 2026 through June 30, 2027.

9. Subparagraph 21.2 of the Contract is hereby amended to read as follows:

21.2 Allowable Costs

During the term of this Contract, COUNTY shall pay CONTRACTOR monthly in arrears, for actual allowable costs incurred and paid by CONTRACTOR pursuant to this Contract, as defined in Title 2 CFR Part 200, or Title 48 CFR Section 31.2 as applicable, or as approved by ADMINISTRATOR. However, COUNTY, at its sole discretion, may pay CONTRACTOR for anticipated allowable costs that will be incurred by CONTRACTOR for the month of June during the term of the contract, during the month of such anticipated expenditure.

10. Paragraph 32 of the Contract is hereby amended to read as follows:

32. SECURITY

Contractor shall abide by the requirements in Attachments B, C, D, E, and F attached hereto and incorporated by reference.

11. Subparagraph 35.4 is hereby added to the Contract as follows:

35.4 Emergency Publicity & Outreach: In response to natural disasters and local emergencies, at the direction of the COUNTY, CONTRACTOR shall assist the COUNTY with publicity of COUNTY provided emergency benefits informational materials and messaging, to provide CONTRACTOR's clientele with helpful emergency benefits and resource information during emergencies.

12. Paragraph 43 of the Contract is hereby amended to read as follows:

43. COOPERATIVE CONTRACT

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

43.2   The provisions and pricing of this Contract may be extended, at the option of Contractor, to any Municipal, County, Public Utility, Hospital, Educational Institution, or any other non-profit or governmental organization (the "Cooperative Program"). Parties in a Cooperative Program wishing to use this Contract will be responsible for issuing their own purchase documents / price agreements, providing for their own acceptance, and making any subsequent payments. Contractor shall be required to include in any agreement entered into with another agency or entity that is entered into pursuant to the provisions and pricing of this Contract a clause that binds the parties to the agreement to "indemnify, defend with counsel approved in writing by the County of Orange, California ("County"), and hold County, its elected and appointed officials, officers, employees, agents and those special districts and

agencies which County's Board of Supervisors acts as the governing Board ("County Indemnitees") harmless from any claims, demands or liability of any kind or nature, including but not limited to personal injury or property damage, arising from or related to the services, products or other performance provided" under the agreement. Failure to so include this clause voids the Contract's extension to a Cooperative Program and will be considered a material breach of this Contract and grounds for immediate Contract termination. The cooperative entities are responsible for obtaining all certificates of insurance and bonds required. The County of Orange makes no guarantee of usage by other users of this Contract.

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

13. Paragraph 3 of Attachment A of the Contract is hereby amended to read as follows:

3. <u>OUTCOME OBJECTIVES</u>:

3.1   CONTRACTOR shall meet the following performance goals for PSEP:

3.1.1   Seventy-five percent (75%) of enrolled PARTICIPANTS shall be placed in employer worksites.

3.1.2   Thirty percent (30%) of all placements will be at public or non-profit sector worksites.

3.1.3   Sixty percent (60%) of PARTICIPANTS will obtain unsubsidized employment within sixty (60) days of completing PSEP placement. CONTRACTOR and ADMINISTRATOR may mutually agree to extend this time frame if there is documentation of pending employment due to the hiring process.

3.2   CONTRACTOR shall meet the following performance goals for WEX:

3.2.1   Seventy-five percent (75%) of enrolled PARTICIPANTS shall be placed in worksites.

3.2.2   Eighty percent (80%) of exiting PARTICIPANTS will obtain unsubsidized employment within thirty (30) days of completing WEX placement.

3.3   CONTRACTOR shall meet the following performance goals for VTR:

3.3.1   Seventy-five percent (75%) of enrolled PARTICIPANTS shall be placed in a training program.

3.3.2   Sixty percent (60%) of PARTICIPANTS will obtain unsubsidized employment or subsidized employment within thirty (30) days of completing VTR program. CONTRACTOR and ADMINISTRATOR may mutually agree to extend to sixty (60) days when certification is delayed or pending employment due to hiring process.

14. Subparagraph 5.8 of Attachment A of the Contract is hereby amended to read as follows:

5.8   CONTRACTOR shall utilize PARTICIPANTS' confidential WTW Assessment report provided by ADMINISTRATOR for each referral to evaluate a PARTICIPANTS' abilities, skills, and interests for employment and training.

15. Subparagraph 5.14.1 of Attachment A of the Contract is hereby amended to read as follows:

5.14.1   Opportunity for permanent employment at the end of the subsidized period or vocational training period;

16. Subparagraph 6.3.3 of Attachment A of the Contract is hereby amended to read as follows:

6.3.3   Utilize accredited vocational training providers that are approved by WIOA and/or by ADMINISTRATOR.

17. Subparagraph 6.3.8 is hereby added to Attachment A of the Contract as follows:

6.3.8   Contractor shall assist PARTICIPANTs exiting VT program with obtaining subsidized employment opportunities, developing subsidized employment worksites in the area of training when necessary.

18. Subparagraph 9.2 of Attachment A of the Contract is hereby amended to read as follows:

9.2   CONTRACTOR shall provide services, pursuant to rent free license agreement(s) with the COUNTY, at the following COUNTY facilities, or as determined by COUNTY:

Anaheim Regional Center
3320 E. La Palma Ave
Anaheim, CA 92806

Laguna Hills Regional Center
23330 Moulton Pkwy
Laguna Hills, CA 92653

Santa Ana Regional Center

1928 S. Grand Ave

Santa Ana, CA 92705

19. Paragraph 10 of Attachment A of the Contract is hereby amended to read as follows:

10. <u>REPORTING REQUIREMENTS</u>

10.1 Comply with data verification requirements per ADMINISTRATOR.

10.2 Immediately implement and adhere to future policy revisions and changes or enhancements in procedures and processes pertaining to submission and reporting requirements.

10.3 Use the most current templates provided by ADMINISTRATOR.

10.4 Implement a quality control process to ensure integrity of all reports submitted to ADMINISTRATOR.

10.5 Provide by the tenth (10th) calendar day of each month, a status report for the preceding month, in a format approved by ADMINISTRATOR. Status reports shall include, but are not limited to, the following:

10.5.1 Total number of referrals received from ADMINISTRATOR and referral outcomes.

10.5.2 Caseload movement: total number of PARTICIPANTS enrolled, participating, exiting, and completing job placements or programs.

10.5.3 Total number of referrals returned to ADMINISTRATOR prior to placement.

10.5.4 List of PARTICIPANTS who obtained unsubsidized employment within thirty (30) and/or sixty (60) calendar days of completing the applicable activity, or otherwise agreed timeline requested by ADMINISTRATOR.

10.5.5 Updated information on the activity status of the referrals and PARTICIPANT attendance issues.

10.5.6 List of issued incentive vouchers including PARTICIPANT name, issuance date, and any related information requested by ADMINISTRATOR.

10.5.7 Surveys requested by ADMINISTRATOR.

10.5.8 First day of attendance reporting: CONTRACTOR shall report the first day's attendance for those PARTICIPANTS scheduled to attend Employment Services, in a format approved by ADMINISTRATOR. Attendance shall be provided to ADMINISTRATOR within three (3) business days of the first day of the Employment Services activity.

20. Paragraph 12 of Attachment A of the Contract is hereby amended to read as follows:

12.1 The annual budget for services provided pursuant to Attachment A of this Contract is set forth as follows:

STAFFING AND BENEFITS:

STAFFING	Position Type [1]	Maximum Hourly Rate [2]	FTEs [3]	Amount
Program Director	A	60.82	0.14	
Project Accountant	A	40.87	0.14	
Training Manager	A	43.27	0.14	
Subcontract Manager	A	43.27	0.14	
Quality Assurance Manager	A	43.27	0.14	
Project Manager	A	47.50	0.14	
Program Manager	D	43.27	0.14	
Human Resources Manager	A	43.27	0.14	
Program Supervisor	D	34.50	1.00	
Human Resources Specialist	A	25.00	1.00	
Job Developer (PSEP)	D	27.43	2.00	
Job Developer (WEX)	D	27.43	2.00	
Job Developer (VTR)	D	27.43	2.00	
Quality Assurance Specialist	D	27.43	1.00	
Administrative Assistant	A	20.44	1.00	
Account Specialist	D	27.43	2.00	

Staffing Subtotal $650,731

EMPLOYEE BENEFITS [4]
(27.22%) $143,723

TOTAL STAFFING & EMPLOYEE BENEFITS	$794,454
TOTAL SERVICES AND SUPPLIES[5]	$2,806,469
TOTAL OPERATING EXPENSES[6]	$127,232
SUBTOTAL STAFFING AND BENEFITS, SERVICES AND SUPPLIES, AND OPERATING EXPENSES	$3,728,155
INDIRECT COSTS (9.68%)[7]	$102,008
PROFIT	$80,907
TOTAL LINE ITEM ANNUAL BUDGET	$3,911,070

[1] Position Types are classified as "D" for Direct or "A" for Administrative. Direct services positions include staff who are integral to service delivery and may include staff who provide direct face-to-face service to clients and/or staff who supervise/manage direct service personnel. Administrative positions include staff that support service delivery and whose activities and functions can be directly allocated to the program.

[2] Maximum hourly rate which will be permitted during the term of this Contract; employees may be paid at less than maximum hourly rate.

[3] For hourly employees, Full-Time Equivalent (FTE) is defined as the amount of time (stated as a percentage) the position will be providing services under the terms of this Contract. This percentage is based upon a 40-hour work week. For salaried employees, FTE is defined as the amount of time (stated as a percentage) the position will be paid for under the terms of this Contract, regardless of the number of hours actually worked.

[4] Employee Benefits include Medical, Dental, Life and Long-Term/Short-Term Disability Insurance; 401(k) Contributions; Workers' Compensation; Tuition Reimbursement; Vacation Paid Time Off (PTO) and expense for accrued vacation time payout, for a separated employee, limited to the actual vacation time accrued during the fiscal year in which the expense is claimed, minus the actual vacation time used by the employee during said fiscal year. The overall benefit rate shall not exceed 27.22% of the actual salary expense claimed.

(5) Services and supplies shall include Audit, VTR, WEX, WEX Post Placement Incentives, PSEP, PSEP Post Placement Incentives, Office Expense, Program Expense, Telephone, Mileage, Advertising. Mileage is limited to the amount allowed by IRS.

(6) Operating expenses shall include Facility Lease/Rental, Equipment Lease/Rental, Insurance, Payroll, Staff Development, Travel.

(7) Indirect cost includes administrative cost not directly charged to the program including common costs associated with the efforts of staff overhead that support projects, professional services, proprietary workforce tools and materials, call/video conferencing, and other miscellaneous items. Indirect costs are based on 9.68% of CONTRACTOR's subtotal direct cost (Staffing, Employee Benefits, Supplies, Operating Expenses, WEX Payroll Expenses, WEX Placement Incentives; PSEP Payroll Expenses, and PSEP Placement Incentives). In the event the indirect cost rate is reduced, the reduction shall be afforded to ADMINISTRATOR and the budget amended accordingly. CONTRACTOR shall provide notification to ADMINISTRATOR of any changes in the rate.

12.2 Expenses for extra pay, including but not limited to, overtime, stipends, bonuses, staff incentives, severance pay, etc. shall not be eligible for reimbursement under this Contract unless authorized in writing by ADMINISTRATOR. Such authorization shall be considered as an exception and may be approved, on a case-by-case basis, at the sole discretion of ADMINISTRATOR.

12.3 CONTRACTOR and ADMINISTRATOR may agree, subject to advance written notice, to add, delete or modify line items and/or amounts and/or the number and type of FTE positions without changing COUNTY's maximum funding obligation as stated in Subparagraph 21.1 of this Contract or reducing the level of service to be provided by CONTRACTOR. Further, in accordance with Subparagraph 42.4 of this Contract, in the event ADMINISTRATOR reduces the maximum funding obligation as stated in Subparagraph 21.1, CONTRACTOR and ADMINISTRATOR may mutually agree in writing to proportionately reduce the service goals as set forth in this Attachment. Failure to obtain advance written approval for any proposed Budget Modification Request may result in disallowance of reimbursement for those costs.

12.4 In the event the budget shown in Subparagraph 12.1 of this Attachment is modified, the modified budget shall remain in effect for the remainder of the contract term, unless superseded by subsequent budget modification(s) that have been approved in writing by

ADMINISTRATOR. For example, if Budget Modification #1 is approved on August 15, 2022, the modified budget will remain in effect until Budget Modification #2 is requested and approved in writing. The annual budget beginning on July 1st of each Contract year shall be identical to the most recently modified annual budget.

21. Attachment D of the Contract is hereby replaced in its entirety and attached as follows.

22. Attachment E of the Contract is hereby replaced in its entirety and attached as follows.

23. Attachment F is hereby added to the Contract and is attached as follows.

24. The Parties agree that separate copies of this Amendment may be signed by each of the Parties, and this Amendment will have the same force and effect as if the original had been signed by all Parties.

25. All other terms and conditions of the Contract shall remain the same and in full force and in effect.

IN WITNESS WHEREOF, the Parties hereto have executed this Amendment Two to Contract on the date set forth opposite their signatures. If Contractor is a corporation, Contractor shall provide two signatures as follows: 1) the first signature must be either the Chairman of the Board, the President, or any Vice President; 2) the second signature must be that of the Secretary, an Assistant Secretary, the Chief Financial Officer, or any Assistant Treasurer. In the alternative, a single corporate signature is acceptable when accompanied by a corporate resolution or by-laws demonstrating the legal authority of the signature to bind the company.

Contractor: ARBOR E&T, LLC DBA EQUUS WORKFORCE SOLUTIONS

Cameron Tovey

_____
Print Name

Chief Financial Officer

_____
Title

DocuSigned by:

Cameron Tovey

8039B33A12A84AC...
_____
Signature

1/9/2025 | 6:38:17 PM EST
_____
Date

_____
Print Name

_____
Title

_____
Signature

_____
Date

County of Orange, a political subdivision of the State of California

Deputized Designee Signature:

_____
Print Name

Deputy Purchasing Agent
_____
Title

_____
Signature

_____
Date

APPROVED AS TO FORM
COUNTY COUNSEL
COUNTY OF ORANGE, CALIFORNIA

Carolyn Frost

_____
Print Name

Deputy County Counsel
_____
Title

DocuSigned by:

Carolyn S. Frost

D3AB98D76D0B425...
_____
Signature

1/9/2025 | 3:40:54 PM PST
_____
Date

WDM0922-A2   Page 19 of 19   January 9, 2025

ATTACHMENT D

COUNTY OF ORANGE INFORMATION TECHNOLOGY SECURITY PROVISIONS

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

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

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

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

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

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

County may require all Contractor personnel, subcontractors, and affiliates approved by County to perform work under this Contract to execute a confidentiality and non-disclosure agreement concerning access protection and data security in the form provided by County. County shall authorize, and Contractor shall issue, any necessary information-access mechanisms, including access IDs and passwords, and in no event shall Contractor permit any such mechanisms to be shared or used by other than the individual Contractor personnel, subcontractor, or affiliate to whom issued. Contractor shall provide each Contractor personnel, subcontractors, or affiliates with only such level of access as is required for such individual to perform his or her assigned tasks and functions.

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

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

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

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

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

Contractor personnel and/or subcontractor personnel and affiliates approved by County to perform work under this Contract may use or disclose County personal and confidential information only as permitted in this Contract. Any other use or disclosure requires express approval in writing by the County of Orange. No Contractor personnel and/or subcontractor personnel or affiliate shall duplicate, disseminate, market, sell, or disclose County personal and confidential information except as allowed in this Contract. Contractor personnel and/or subcontractor personnel or affiliate who access, disclose, market, sell, or use County personal and confidential information in a manner or for a purpose not authorized by this Contract may be subject to civil and criminal sanctions contained in applicable federal and state statutes.

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

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

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

5. **Enhanced Security Measures:** County may, in its discretion, designate certain areas, facilities, or solution systems as ones that require a higher level of security and access control. County shall notify Contractor in writing reasonably in advance of any such designation becoming effective. Any such notice shall set forth, in reasonable detail, the enhanced security or access-control procedures, measures, or requirements that Contractor shall be required to implement and enforce, as well as the date on which such procedures and measures shall take effect. Contractor shall and shall cause Contractor personnel and subcontractors to fully comply with and abide by all such enhanced security and access measures and procedures as of such date.

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

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

b) **Contractor and the use of Email:** Contractor, including Contractor's employees and subcontractors, that are provided a County email address must only use the County email system for correspondence of County business. Contractor, including Contractor's employees and subcontractors, must not access or use personal, non-County Internet (external) email systems from County networks and/or County computing devices. If at any time Contractor's performance under this Contract requires such access or use, Contractor must submit a written request to County with justification for access or use of personal, non-County Internet (external) email systems from County networks and/or computing devices and obtain County's express prior written approval.

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

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

8. Security Breach Notification: In the event Contractor becomes aware of any act, error or omission, negligence, misconduct, or security incident including unsecure or improper data disposal, theft, loss, unauthorized use and disclosure or access, that compromises or is suspected to compromise the security, availability, confidentiality, and/or integrity of County data or the physical, technical, administrative, or organizational safeguards required under this Contract that relate to the security, availability, confidentiality, and/or integrity of County data, Contractor shall, at its own expense, (1) immediately (or within 24 hours of potential or suspected breach), notify the County's Chief Information Security Officer and County Privacy Officer of such occurrence; (2) perform a root cause analysis of the actual, potential, or suspected breach; (3) provide a remediation plan that is

acceptable to County within 30 days of verified breach, to address the occurrence of the breach and prevent any further incidents; (4) conduct a forensic investigation to determine what systems, data, and information have been affected by such event; and (5) cooperate with County and any law enforcement or regulatory officials investigating such occurrence, including but not limited to making available all relevant records, forensics, investigative evidence, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by County and/or any law enforcement or regulatory officials, and (6) perform or take any other actions required to comply with applicable law as a result of the occurrence (at the direction of County).

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

In the case of a breach, Contractor shall provide third-party credit and identity monitoring services to each of the affected individuals for the period required to comply with applicable law, or, in the absence of any legally required monitoring services, for no less than twelve (12) months following the date of notification to such individuals.

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

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

9. **Security Audits:** Contractor shall maintain complete and accurate records relating to its system and Organization Controls (SOC) Type II audits or equivalent's data protection practices, internal and external audits, and the security of any of County-hosted content, including any confidentiality, integrity, and availability operations (data hosting, backup,

disaster recovery, external dependencies management, vulnerability testing, penetration testing, patching, or other related policies, practices, standards, or procedures).

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

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

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

10. Business Continuity and Disaster Recovery (BCDR):

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

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

All data and/or systems and technology provided by the Contractor internally and through third-party vendors shall have resiliency and redundancy capabilities to achieve high

availability and data recoverability. Contractor Systems shall be designed, where practical and possible, to ensure continuity of service(s) in the event of a disruption or outage.

ATTACHMENT E

STATE PRIVACY AND SECURITY PROVISIONS

1. **DEFINITIONS**

    For the purpose of this Agreement, the following terms mean:

    a. "**Assist in the Administration of the Program**" means performing administrative functions on behalf of programs, such as determining eligibility for, or enrollment in, and collecting PII for such purposes, to the extent such activities are authorized by law.

    b. "**Breach**" refers to actual loss, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to PII, whether electronic, paper, verbal, or recorded.

    c. "**Contractor Staff**" means those employees of the contractor/subcontractor, vendors and agents performing any functions for the county that require access to and/or use of PII and that are authorized by the county to access and use PII.

    d. "**PII**" is personally identifiable information that is obtained through the MEDS or IEVS on behalf of the programs and can be used alone, or in conjunction with any other reasonably available information, to identify a specific individual. The PII includes, but is not limited to, an individual's name, social security number, driver's license number, identification number, biometric records, date of birth, place of birth, or mother's maiden name. The PII may be electronic, paper, verbal, or recorded.

    e. "**Security Incident**" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PII, or interference with system operations in an information system which processes PII that is under the control of the county or county's Statewide Automated Welfare System (SAWS) Consortium, or CalWIN (California Welfare Information Network), or under the control of a contractor, subcontractor or vendor of the county, on behalf of the county.

    f. "**Secure Areas**" means any area where:
        i.   Contractor Staff assist in the administration of their program;
        ii. Contractor Staff use or disclose PII; or
        iii. PII is stored in paper or electronic format.

2. **PRIVACY AND CONFIDENTIALITY**

a. The County staff, contractors, subcontractors and vendors, covered by this Agreement may use or disclose PII only as permitted in this Agreement and only to assist in the administration of programs in accordance with 45 CFR § 205.50 et. seq and Welfare and Institutions Code section 10850, and Section 14100.2 of the Welfare and Institutions Code, Section 431.300 et. Seq. of Title 42 Code of Federal Regulations, or as authorized or required by law. Disclosures, which are authorized or required by law, such as a court order, or are made with the explicit written authorization of the individual, who is the subject of the PII, are allowable. Any other use or disclosure of PII requires the express approval in writing by County of Orange. No Contractor Staff shall duplicate, disseminate or disclose PII except as allowed in this Agreement.

b. Pursuant to this Agreement, Contractor Staff may only use PII to perform administrative functions related to administering their respective programs.

c. Access to PII shall be restricted to Contractor Staff who need to perform their official duties to assist in the administration of their respective programs.

d. Contractor Staff who access, disclose or use PII in a manner or for a purpose not authorized by this Agreement may be subject to civil and criminal sanctions contained in applicable federal and state statutes.

3. **PERSONNEL CONTROLS**

The County agrees to advise Contractor Staff, who have access to PII, of the confidentiality of the information, the safeguards required to protect the information, and the civil and criminal sanctions for non-compliance contained in applicable federal and state laws. For that purpose, the Contractor shall implement the following personnel controls:

a. **Employee Training.** Train and use reasonable measures to ensure compliance with the requirements of this Agreement by Contractor Staff, including, but not limited to:
   i. Provide initial privacy and security awareness training to each new Contractor Staff within thirty (30) days of employment and;
   ii. Thereafter, provide annual refresher training or reminders of the privacy and security safeguards in this Agreement to all Contractor Staff. Three (3) or more security reminders per year are recommended;
   iii. Maintain records indicating each Contractor Staff's name and the date on which the privacy and security awareness training was completed;
   iv. Retain training records for a period of three (3) years after completion of the training.

b. **Employee Discipline.**
   i. Provide documented sanction policies and procedures for Contractor Staff who fail to comply with privacy policies and procedures or any provisions of these requirements.
   ii. Sanction policies and procedures shall include termination of employment

when appropriate.

c. **Confidentiality Statement**. Ensure that all Contractor Staff, accessing, using or disclosing PII, sign a confidentiality statement (provided by the County). The statement shall be signed by Contractor staff prior to accessing PII and annually thereafter. Signatures may be physical or electronic. The signed statement shall be retained for a period of three (3) years.

    The statement shall include at a minimum:
i.   General Use;
ii.   Security and Privacy Safeguards;
iii.   Unacceptable Use; and
iv.   Enforcement Policies.

d. **Background Screening.**
i.   Conduct a background screening of a Contractor Staff before they may access PII.
ii.   The background screening should be commensurate with the risk and magnitude of harm the employee could cause. More thorough screening shall be done for those employees who are authorized to bypass significant technical and operational security controls.
iii.   The Contractor shall retain each Contractor Staff's background screening documentation for a period of three (3) years following conclusion of employment relationship.

4.   <u>MANAGEMENT OVERSIGHT AND MONITORING</u>

To ensure compliance with the privacy and security safeguards in this Agreement the County shall perform the following:

a. Conduct periodic privacy and security reviews of work activity by Contractor Staff, including random sampling of work product. Examples include, but are not limited to, access to case files or other activities related to the handling of PII.

b. The periodic privacy and security reviews must be performed or overseen by management level personnel who are knowledgeable and experienced in the areas of privacy and information security in the administration of their program, and the use or disclosure of PII.

5.   <u>INFORMATION SECURITY AND PRIVACY STAFFING</u>

The Contractor agrees to:

a. Designate information security and privacy officials who are accountable for compliance with these and all other applicable requirements stated in this Agreement.

b. Provide County with applicable contact information for these designated individuals. Any changes to this information should be reported to County within ten (10) days.

c. Assign staff to be responsible for administration and monitoring of all security related controls stated in this Agreement.

6. <u>PHYSICAL SECURITY</u>

The Contractor shall ensure PII is used and stored in an area that is physically safe from access by unauthorized persons at all times. The Contractor agrees to safeguard PII from loss, theft, or inadvertent disclosure and, therefore, agrees to:

a. Secure all areas of the Contractor's facilities where Contractor Staff assist in the administration of their program and use, disclose, or store PII.

b. These areas shall be restricted to only allow access to authorized individuals by using one or more of the following:
    i.   Properly coded key cards
    ii.   Authorized door keys
    iii. Official identification

c. Issue identification badges to Contractor Staff.

d. Require Contractor Staff to wear these badges where PII is used, disclosed, or stored.

e. Ensure each physical location, where PII is used, disclosed, or stored, has procedures and controls that ensure an individual who is terminated from access to the facility is promptly escorted from the facility by an authorized employee and access is revoked.

f. Ensure there are security guards or a monitored alarm system at all times at the Contractor facilities and leased facilities where five hundred (500) or more individually identifiable records of PII is used, disclosed or stored. Video surveillance are recommended.

g. Ensure data centers with servers, data storage devices, and/or critical network infrastructure involved in the use, storage, and/or processing of PII have perimeter security and physical access controls that limit access to only authorized Contractor Staff. Visitors to the data center area must be escorted at all times by authorized Contractor Staff.

h. Store paper records with PII in locked spaces, such as locked file cabinets, locked file rooms, locked desks, or locked offices in facilities which have multi-use functions in one building in work areas that are not securely segregated from each other. It is recommended that all PII be locked up when unattended at any time, not just within

multi-use facilities.

i. The Contractor shall have policies that include, based on applicable risk factors, a description of the circumstances under which the Contractor Staff can transport PII, as well as the physical security requirements during transport. A Contractor that chooses to permit its staff to leave records unattended in vehicles must include provisions in its policies to ensure the PII is stored in a non-visible area such as a trunk, that the vehicle is locked, and under no circumstances permit PII be left unattended in a vehicle overnight or for other extended periods of time.

j. The Contractor shall have policies that indicate Contractor Staff are not to leave records with PII unattended at any time in airplanes, buses, trains, etc., including baggage areas. This should be included in training due to the nature of the risk.

k. Use all reasonable measures to prevent non-authorized personnel and visitors from having access to, control of, or viewing PII.

7. **TECHNICAL SECURITY CONTROLS**

a. **Workstation/Laptop Encryption.** All workstations and laptops, which use, store and/or process PII, must be encrypted using a FIPS 140-2 certified algorithm 128 bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk. It is encouraged, when available and when feasible, that the encryption be 256 bit.

b. **Server Security.** Servers containing unencrypted PII must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review. It is recommended to follow the guidelines documented in the latest revision of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

c. **Minimum Necessary.** Only the minimum necessary amount of PII required to perform required business functions may be accessed, copied, downloaded, or exported.

d. **Mobile Device and Removable Media.** All electronic files, which contain PII data, must be encrypted when stored on any mobile device or removable media (i.e., USB drives, CD/DVD, smartphones, tablets, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm 128 bit or higher, such as AES. It is encouraged, when available and when feasible, that the encryption be 256 bit.

e. **Antivirus Software.** All workstations, laptops and other systems, which process and/or store PII, must install and actively use an antivirus software solution. Antivirus software should have automatic updates for definitions scheduled at least daily.

f. **Patch Management.**
    i.   All workstations, laptops and other systems, which process and/or store PII, must have critical security patches applied, with system reboot if necessary.
    ii. There must be a documented patch management process that determines installation timeframe based on risk assessment and vendor recommendations.
    iii. At a maximum, all applicable patches deemed as critical must be installed within thirty (30) days of vendor release. It is recommended that critical patches which are high risk be installed within seven (7) days.
    iv. Applications and systems that cannot be patched within this time frame, due to significant operational reasons, must have compensatory controls implemented to minimize risk.

g. **User IDs and Password Controls.**
    i.   All users must be issued a unique username for accessing PII.
    ii.   Username must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee within twenty-four (24) hours. Note: Twenty-four (24) hours is defined as one (1) working day.
    iii. Passwords are not to be shared.
    iv.   Passwords must be at least eight (8) characters.
    v.   Passwords must be a non-dictionary word.
    vi.   Passwords must not be stored in readable format on the computer or server.
    vii. Passwords must be changed every ninety (90) days or less.
    viii. Passwords must be changed if revealed or compromised.
    ix.   Passwords must be composed of characters from at least three (3) of the following four (4) groups from the standard keyboard:
          A. Upper case letters (A-Z)
          B. Lower case letters (a-z)
          C. Arabic numerals (0-9)
          D. Special characters (!,@,#, etc.)

h. **Data Destruction.** When no longer needed, all PII must be cleared, purged, or destroyed consistent with NIST SP 800-88, Guidelines for Media Sanitization, such that the PII cannot be retrieved.

i. **System Timeout.** The systems providing access to PII must provide an automatic timeout, requiring re-authentication of the user session after no more than twenty (20) minutes of inactivity.

j. **Warning Banners.** The systems providing access to PII must display a warning banner stating, at a minimum:
    i.   Data is confidential;
    ii. Systems are logged;
    iii. System use is for business purposes only, by authorized users; and
    iv. Users shall log off the system immediately if they do not agree with these requirements.

    k. **System Logging.**

        i.   The systems which provide access to PII must maintain an automated audit trail that can identify the user or system process which initiates a request for PII or alters PII.

        ii.   The audit trail shall:

            A. Be date and time stamped;

            B. Log both successful and failed accesses;

            C. Be read-access only; and

            D. Be restricted to authorized users.

        iii.   If PII is stored in a database, database logging functionality shall be enabled.

        iv.   Audit trail data shall be archived for at least three (3) years from the occurrence.

    l. **Access Controls.** The system providing access to PII shall use role-based access controls for all user authentications, enforcing the principle of least privilege.

    m. **Transmission Encryption.**

        i.   All data transmissions of PII outside of a secure internal network must be encrypted using a Federal Information Processing Standard (FIPS) 140-2 certified algorithm that is 128 bit or higher, such as Advanced Encryption Standard (AES) or Transport Layer Security (TLS). It is encouraged, when available and when feasible, that 256 bit encryption be used.

        ii.   Encryption can be end to end at the network level, or the data files containing PII can be encrypted.

        iii.   This requirement pertains to any type of PII in motion such as website access, file transfer, and email.

    n. **Intrusion Prevention.** All systems involved in accessing, storing, transporting, and protecting PII, which are accessible through the Internet, must be protected by an intrusion detection and prevention solution.

8.   <u>AUDIT CONTROLS</u>

    a. **System Security Review.**

        i.   The Contractor must ensure audit control mechanisms are in place.

        ii.   All systems processing and/or storing PII must have at least an annual system risk assessment/security review that ensures administrative, physical, and technical controls are functioning effectively and provide an adequate level of protection.

        iii.   Reviews should include vulnerability scanning tools.

    b. **Log Reviews.** All systems processing and/or storing PII must have a process or automated procedure in place to review system logs for unauthorized access.

c. **Change Control.** All systems processing and/or storing PII must have a documented change control process that ensures separation of duties and protects the confidentiality, integrity and availability of data.

d. **Anomalies.** When the County or DHCS suspects MEDS usage anomalies, the County will work with Contractor to investigate the anomalies and report conclusions of such investigations and remediation to California Department of Social Services (CDSS).

9. BUSINESS CONTINUITY / DISASTER RECOVERY CONTROLS

a. **Emergency Mode Operation Plan.** The Contractor must establish a documented plan to enable continuation of critical business processes and protection of the security of PII kept in an electronic format in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than twenty-four (24) hours.

b. **Data Centers.** Data centers with servers, data storage devices, and critical network infrastructure involved in the use, storage and/or processing of PII, must include environmental protection such as cooling, power, and fire prevention, detection, and suppression.

c. **Data Backup and Recovery Plan.**

   i. The Contractor shall have established documented procedures to backup PII to maintain retrievable exact copies of PII.
   ii. The documented backup procedures shall contain a schedule which includes incremental and full backups.
   iii. The procedures shall include storing backups offsite.
   iv. The procedures shall ensure an inventory of backup media.
   v. The Contractor shall have established documented procedures to recover PII data.
   vi. The documented recovery procedures shall include an estimate of the amount of time needed to restore the PII data.
   vii. It is recommended that the Contractor periodically test the data recovery process.

10. PAPER DOCUMENT CONTROLS

a. **Supervision of Data.** The PII in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information may be observed by an individual not authorized to access the information.

b. **Data in Vehicles.** The Contractor shall have policies that include, based on applicable risk factors, a description of the circumstances under which the Contractor Staff can transport PII, as well as the physical security requirements during transport. A Contractor that chooses to permit its staff to leave records unattended in vehicles must include provisions in its policies to ensure the PII is stored in a non-visible area such as a trunk, that the vehicle is locked, and under no circumstances permit PII be left unattended in a vehicle overnight or for other extended periods of time.

c. **Public Modes of Transportation.** The PII in paper form shall not be left unattended at any time in airplanes, buses, trains, etc., including baggage areas. This should be included in training due to the nature of the risk.

d. **Escorting Visitors.** Visitors to areas where PII is contained shall be escorted, and PII shall be kept out of sight while visitors are in the area.

e. **Confidential Destruction.** PII must be disposed of through confidential means, such as cross-cut shredding or pulverizing.

f. **Removal of Data.** The PII must not be removed from the premises of Contractor except for identified routine business purposes or with express written permission of HHS.

g. **Faxing.**

   i. Faxes containing PII shall not be left unattended and fax machines shall be in secure areas.
   ii. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them and notify the sender.
   iii. Fax numbers shall be verified with the intended recipient before sending the fax

h. **Mailing.**
   i. Mailings containing PII shall be sealed and secured from damage or inappropriate viewing of PII to the extent possible.
   ii. Mailings that include five hundred (500) or more individually identifiable records containing PII in a single package shall be sent using a tracked mailing method that includes verification of delivery and receipt, unless the Contractor obtains prior written permission from HHS to use another method.

11. <u>**NOTIFICATION AND INVESTIGATION OF BREACHES AND SECURITY INCIDENTS**</u>

During the term of this Agreement, the County agrees to implement reasonable systems for the discovery and prompt reporting of any Breach or Security Incident, and to take the following steps:

a. **Initial Notice to HHS:**
   i. The Contractor will provide initial notice to the County. The Contractor agrees to perform the following incident reporting to County.
   ii. Immediately upon discovery of a suspected security incident that involves data provided to Contractor by County, the Contractor will notify the County by email or telephone.
   iii. Within one working day of discovery, the Contractor will notify the County by email or telephone of unsecured PII, if that PII was, or is, reasonably believed to have been accessed or acquired by an unauthorized person, any suspected security incident, intrusion, or unauthorized access, use, or disclosure of PII in violation of this Agreement, or potential loss of confidential data affecting this Agreement. Notice shall be made by contacting the County as provided in this agreement, including all information known at the time.
   iv. A breach shall be treated as discovered by the Contractor as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach), who is an employee, officer or other agent of the Contractor.
   v. Upon discovery of a breach, security incident, intrusion, or unauthorized access, use, or disclosure of PII, the Contractor shall take:
      A. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and
      B. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

b. **Investigation and Investigative Report.** The Contractor shall immediately investigate breaches and security incidents involving PII. The Contractor will cooperate with the County during this investigation. Within seventy-two (72) hours of discovery, the Contractor shall provide new or updated information if available to County. The updated report shall include any other applicable information related to the breach or security incident known at that time. The Contractor shall provide status update to County on a regular basis as agreed upon.

The Contractor shall provide to County all specific and pertinent information about the Breach, including copies of any reports conducted by the Contractor or on behalf of the Contractor. The Contractor shall waive any assertion of privilege in relation to such reports. Such information and/or reports shall be provided to County without unreasonable delay and in no event later than fifteen (15) calendar days the Contractor have such information and/or report.

c. **Complete Report.** The complete report of the investigation shall include an assessment of all known factors relevant to the determination of whether a breach occurred under applicable provisions of the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, the Information Protection Act, or other applicable law.

The report shall include a Corrective Action Plan (CAP) which includes, at a minimum, detailed information regarding the mitigation measures taken to halt and/or contain the improper use or disclosure.

If County requests additional information related to the incident, the Contractor shall make reasonable efforts to provide County with such information. County will review report and determine whether a breach occurred and whether individual notification is required. County will maintain the final decision making over a breach determination.

d. **Notifications of Individuals**. When applicable state or federal law requires notification to individuals of a breach or unauthorized disclosure of their PII, the County will make the decision to either notify clients or have the Contractor give notice. If the Contractor shall give the notice, it would be subject to the following provisions:

   i. If the cause of the breach is attributable to the Contractor or its subcontractors, agents or vendors, the Contractor shall pay any costs of such notifications, as well as any and all costs associated with the breach. If there are any questions as to whether the County or the Contractor is responsible for the breach, the County and the Contractor shall jointly determine responsibility for purposes of allocating the costs;

   ii. All notifications (regardless of breach status) regarding the beneficiaries' PII shall comply with the requirements set forth in Section 1798.29 of the California Civil Code and Section 17932 of Title 42 of the United States Code, inclusive of its implementing regulations, including but not limited to the requirement that the notifications be made without reasonable delay and in no event, later than sixty (60) calendar days from discovery;

   iii. The County has contractual requirement with the California Department of Social Services and California Department of Health Care Services to approve the time, manner and content of any such notifications and their review and approval shall be obtained before notifications are made. Therefore, the Contractor must provide the notifications to County to obtain review and approval prior to notifications are made. If notifications are distributed without State review and approval, secondary follow-up notifications may be required; and

   iv. The County may elect to assume responsibility for such notification from the Contractor.

e. **Responsibility for Reporting of Breaches when Required by State or Federal Law.** If the cause of a breach is attributable to the Contractor or its agents, subcontractors or vendors, the Contractor is responsible for all required reporting of the breach. If the cause of the breach is attributable to the County, the County is responsible for all required reporting of the breach. When applicable law requires the breach be reported to a federal or state agency or that notice be given to media outlets, DHCS (Department of Health Care Services) and CDSS (California Department of Social Services) (if the breach involves MEDS or SSA data), then the Contractor shall coordinate with the County to ensure such reporting is in compliance with applicable law and to prevent duplicate reporting, and to jointly determine responsibility for purposes of allocating

the costs of such reports, if any.

f. **County Contact Information.** The Contractor shall utilize the below contact information to direct all notifications of breach and security incidents to the County. The County reserves the right to make changes to the contact information by giving written notice to the Contractor. Said changes shall not require an amendment to this Agreement or any other agreement into which it is incorporated.

Social Services Agency Contact	County Privacy Officer
County of Orange Social Services Agency Contracts Services 500 N. State College Blvd, Suite 100 Orange, CA 92868 714-541-7785 Karen.Vu@ssa.ocgov.com	Linda Le, CHC, CHPC, CHP County of Orange OCIT - Enterprise Privacy & Cybersecurity 1055 N. Main St, 6th Floor Santa Ana, CA 92701 Email: privacyofficer@ocgov.com securityadmin@ocit.ocgov.com linda.le@ocit.ocgov.com

12. **COMPLIANCE WITH SSA (SOCIAL SECURITY ADMINISTRATION) AGREEMENT**

The County has agreed to comply with applicable privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement (CMPPA) between the SSA and the California Health and Human Services Agency (CHHS), in the Information Exchange Agreement (IEA) between SSA and CDSS, and in the Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with SSA (TSSR). If Contractor have access to the PII data provided by SSA, then Contractor must agree to comply with the applicable privacy and security requirements, which is available upon request.

If there is any conflict between a privacy and security standard in the CMPPA, IEA or TSSR, and a standard in this Agreement, the most stringent standard shall apply. The most stringent standard means the standard which provides the greatest protection to PII.

13. **COMPLIANCE WITH DEPARTMENT OF HOMELAND SECURITY**

AGREEMENT

The County has agreed to comply with substantive privacy and security requirements in the Computer Matching Agreement (CMA) between the Department/Agency of Homeland Security, United States Citizenship and Immigration Services (DHS-USCIS) and CDSS. If Contractor have access to the PII data provided by DHS-USCIS, then Contractor must agree to comply with the applicable privacy and security requirements, which is available upon request.

If there is any conflict between a privacy and security standard in the CMA and a standard in this Agreement, the most stringent standard shall apply. The most stringent standard means the standard which provides the greatest protection to PII.

14.   **CONTRACTOR AGENTS, SUBCONTRACTORS, AND VENDORS**

The Contractor agrees to enter into written agreements with all agents, subcontractors, and vendors that have access to the Contractor's PII. These agreements will impose, at a minimum, the same restrictions and conditions that apply to the Contractor with respect to PII upon such agents, subcontractors, and vendors. These shall include, at a minimum, (1) restrictions on disclosure of PII, (2) conditions regarding the use of appropriate administrative, physical, and technical safeguards to protect PII, and, where relevant, (3) the requirement that any breach, security incident, intrusion, or unauthorized access, use, or disclosure of PII be reported to the Contractor. If the agents, subcontractors, and vendors of the Contractor access data provided to the County by SSA or DHS-USCIS, the Contractor shall also incorporate the Agreement's Exhibits into each subcontract or subaward with agents, subcontractors, and vendors.

15.   **ASSESSMENTS AND REVIEWS**

In order to enforce this Agreement and ensure compliance with its provisions, the Contractor agrees to assist the County (on behalf of CDSS and DHCS) in performing compliance assessments. These assessments may involve compliance review questionnaires, and/or review of the facilities, systems, books, and records of the Contractor, with reasonable notice from the County. Such reviews shall be scheduled at times that take into account the operational and staffing demands. The Contractor agrees to promptly remedy all violations of any provision of this Agreement and certify the same to the County in writing, or to enter into a written CAP (Corrective Action Plan) with the County containing deadlines for achieving compliance with specific provisions of this Agreement.

16.   **ASSISTANCE IN LITIGATION OR ADMINISTRATIVE PROCEEDINGS**

In the event of litigation or administrative proceedings involving the County based upon claimed violations by the Contractor of the privacy or security of PII, or federal or state

laws or agreements concerning privacy or security of PII, the Contractor shall make all reasonable effort to make itself and Contract Workers assisting in the administration of their program and using or disclosing PII available to the County at no cost to the County to testify as witnesses. The County shall also make all reasonable efforts to make itself and any subcontractors, agents, and employees available to the Contractor at no cost to the Contractor to testify as witnesses, in the event of litigation or administrative proceedings involving the Contractor based upon claimed violations by the County of the privacy or security of PII, or state or federal laws or agreements concerning privacy or security of PII.

County of Orange

Information Technology Security Guidelines

ATTACHMENT F

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. All vendors who contract with the County of Orange ("County") shall work cooperatively to assist County in achieving the objectives and abide by the applicable terms under these Guidelines at all times during the term of its contract with County.

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.

County of Orange

Information Technology Security Guidelines

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

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

---

July 3, 2024

County of Orange

Information Technology Security Guidelines

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.

County of Orange

Information Technology Security Guidelines

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.

County of Orange

Information Technology Security Guidelines

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

County of Orange

Information Technology Security Guidelines

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:

County of Orange

Information Technology Security Guidelines

- 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.

County of Orange

Information Technology Security Guidelines

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.

County of Orange

Information Technology Security Guidelines

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.

County of Orange

Information Technology Security Guidelines

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 whitelisting and blacklisting of applications, web sites, and IP addresses.

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

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

2.2.16 Data Loss Prevention

2.2.16.1 Departments 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.

County of Orange

Information Technology Security Guidelines

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

County of Orange

Information Technology Security Guidelines

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.

County of Orange

Information Technology Security Guidelines

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 if applicable. 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

County of Orange

Information Technology Security Guidelines

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.

County of Orange

Information Technology Security Guidelines

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.