



CONTRACT NO. MA-012-22011942

FOR THE PROVISION OF

AMERICAN RESCUE PLAN ACT (ARPA) (H.R. 1319)
SUPPORT OF ORANGE COUNTY HUMAN RELATIONS COMMISSION PROGRAMS AND
SERVICES

BETWEEN

COUNTY OF ORANGE

AND

ORANGE COUNTY HUMAN RELATIONS COUNCIL

<u>CFDA#</u>	<u>FAIN#</u>	<u>PROGRAM/SERVICE TITLE</u>	<u>FUNDING AGENCY</u>
21.027	Pending	American Rescue Plan Act (ARPA) (H.R. 1319)	U.S. Department of the Treasury

Table of Contents

RECITALS..... 6

General Terms and Conditions:..... 9

 A. **Governing Law and Venue:..... 9**

 B. **Entire Contract:..... 9**

 C. **Amendments:..... 9**

 D. **Intentionally left blank..... 9**

 E. **Delivery:..... 9**

 F. **Acceptance Payment:..... 9**

 G. **Warranty:..... 9**

 H. **Patent/Copyright Materials/Proprietary Infringement:..... 10**

 I. **Assignment:..... 10**

 J. **Non-Discrimination:..... 10**

 K. **Termination:..... 10**

 L. **Consent to Breach Not Waiver:..... 11**

 M. **Independent Contractor:..... 12**

 N. **Performance Warranty:..... 12**

 O. **Insurance Requirements:..... 12**

 P. **Changes:..... 15**

 Q. **Change of Ownership/Name, Litigation Status, Conflicts with County Interest:..... 15**

 R. **Force Majeure:..... 16**

 S. **Confidentiality:..... 16**

 T. **Compliance with Laws:..... 17**

 U. **Intentionally left blank..... 17**

 V. **Severability:..... 17**

 W. **Attorney Fees:..... 17**

 X. **Interpretation:..... 17**

 Y. **Employee Eligibility Verification:..... 17**

 Z. **Indemnification:..... 18**

 AA. **Audits/Inspections:..... 18**

 BB. **Contingency of Funds:..... 18**

 CC. **Expenditure Limit:..... 19**

Additional Terms and Conditions:..... 20

 1. **Scope of Contract:..... 20**

 2. **Term of Contract:..... 20**

 3. **Renewal:..... 20**

4. **Headings:**..... 20

5. **Maximum Obligation** 20

6. **Amendments – Changes/Extra Work:**..... 20

7. **Breach of Contract:**..... 20

8. **Conditions Affecting Work:**..... 21

9. **Conflict of Interest – Contractor’s Personnel:** 21

10. **Conflict of Interest – County Personnel:** 21

11. **Service Contract – Follow-On Work:**..... 21

12. **Project Manager, County:** 21

13. **Contractor’s Project Manager and Key Personnel:** 22

14. **Data – Title To:** 22

15. **Licenses:** 23

16. **Disputes – Contract:**..... 23

17. **EDD Independent Contractor Reporting Requirements:**..... 24

18. **Errors and Omissions:**..... 24

19. **Non-Supplantation of Funds:**..... 24

20. **Satisfactory Work:** 25

21. **Access and Records:** 25

22. **Signature in Counterparts:**..... 25

23. **Reports/Meetings:** 25

24. **Subcontracting:**..... 25

25. **Equal Employment Opportunity:** 26

26. **Gratuities:**..... 26

27. **News/Information Release:**..... 26

28. **Notices:**..... 26

29. **Ownership of Documents:** 27

30. **Precedence:**..... 27

31. **Termination – Orderly:** 27

32. **Default – Re-Procurement Costs:**..... 27

33. **County Branding Requirements:** 28

34. **Policies and Procedures:** 29

35. **Security Policies:** 29

36. **Information Access:** 29

37. **Data Security Requirements:** 30

38. **Enhanced Security Measures:** 30

39. **General Security Standards:**..... 30

40. **Security Failures:** 31

41. **Security Breach Notification:** 31

42. **Security Audits:** 32

43. **Debarment:** 33

44. **Lobbying Certification:** 33

45. **Fraud:**..... 33

46. **Fiscal Appropriations:**..... 33

47. **Fiscal Accountability:** 33

48. **Indirect Costs:**..... 34

49. **Dissolution of Entity:**..... 34

50. **Performance Standards:**..... 34

51. **Payments** 36

52. **Budget and Staffing Plan:**..... 37

53. **Modification of Budget and Staffing Plan:** 37

54. **Annual Audit:** 38

55. **Audit Requirements:** 38

56. **Non-Discrimination and Compliance Provisions:** 40

57. **Drug Free Workplace:**..... 41

58. **D-U-N-S Number and Related Information:** **Error! Bookmark not defined.**

59. **Modification of Program Components and Service Levels:**..... 42

60. **Complaint Resolution Process and Grievance Procedures for Participants:** 43

61. **Sectarian Activities:** 43

62. **Policies and Procedures:**..... 43

63. **Sweat-free Code of Conduct:** 43

64. **S.W.A.G:** 43

65. **Corporate Status:**..... 43

66. **Compliance with Other Laws:** 44

67. **Focal Points:** 45

68. **Covenant Against Contingent Fees:** 45

Signature Page **46**

ATTACHMENTS

Attachment A - Scope of Services
Attachment B - Payment/Compensation
Attachment C - Budget and Staffing Plan
Attachment D – Federal Award Identification
Attachment E- County Cybersecurity Policy
Attachment F- Certification of Return or Destruction and Non-Data Breach

EXHIBITS

Exhibit 1 – Drug Free Workplace Certification
Exhibit 2 – Debarment and Suspension Certificate
Exhibit 3 – Certification Regarding Lobbying
Exhibit 4 – Disclosure Form to Report Lobbying
Exhibit 5 – OC Community Resources Contract Reimbursement Policy

Contract No. MA-012-22011942
with
Orange County Human Relations Council
For
American Rescue Plan Act (ARPA) (H.R. 1319)
Support of Orange County Human Relations Commission Programs and Services

This Contract No. MA-012-22011942 for American Rescue Plan Act (ARPA) (H.R. 1319) Support of the Orange County Human Relations Commission (“Orange County Human Relations Commission” or “Commission”) Programs and Services (hereinafter referred to as “Contract”) is made and entered into as of the date fully executed by and between the County of Orange, a political subdivision of the State of California; hereinafter referred to as “County” and Orange County Human Relations Council, D-U-N-S No. 039841668 and SAM Unique Entity ID # TFLRQY5PNT89, a California non-profit corporation, with a place of business at 1801 E. Edinger Ave., Suite 115, Santa Ana, CA 92705 (hereinafter referred to as “Contractor”), with a County and Contractor sometimes referred to as “Party” or collectively as “Parties”.

ATTACHMENTS

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

- Attachment A – Scope of Services
- Attachment B – Payment/Compensation
- Attachment C – Budget Schedule
- Attachment D – Federal Award Identification
- Attachment E- County Cybersecurity Policy
- Attachment F- Certification of Return or Destruction and Non-Data Breach

- Exhibit 1 – Drug Free Workplace Certification
- Exhibit 2 – Debarment and Suspension Certificate
- Exhibit 3 – Certification Regarding Lobbying
- Exhibit 4 – Disclosure Form to Report Lobbying
- Exhibit 5 – OC Community Resources Contract Reimbursement Policy

RECITALS

WHEREAS, Contractor and County are entering into this Contract for American Rescue Plan Act (ARPA) (H.R. 1319)–Support of Orange County Human Relations Commission Programs and Services under a cost reimbursement Contract; and

WHEREAS, County solicited, under Request for Proposal, this Contract for County of Orange OC Community Services as set forth herein, and Contractor represented that it is qualified to provide Support of Orange County Human Relations Commission Programs and Services to the County as further set forth herein; and

WHEREAS, Contractor agrees to provide ARPA (H.R. 1319) Support of Orange County Human Relations Commission Programs and Services to the County as further set forth in the Scope of Service, attached hereto as Attachment A; and

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

WHEREAS, Contractor agrees to manage allotted funding set forth in the Budget and Staffing Plan, attached hereto as Attachment C; and

WHEREAS, Contractor acknowledges and understands information set forth in the Federal Award Identification Information, attached hereto as Attachment D; and

WHEREAS, Contractor agrees to meet the County Cybersecurity Policy requirements set forth and attached hereto as Attachment E; and

WHEREAS, Contractor agrees to meet the Certification of Return or Destruction and Non-Data Breach requirements set forth and attached hereto as Attachment F; and

WHEREAS, the County Board of Supervisors has authorized the OC Community Resources Director or his designee to enter into this ARPA (H.R. 1319) Support of Orange County Human Relations Commission Programs and Services Contract with the Contractor to carry out certain program services and activities for the Fiscal Years 2022-2024.

NOW, THEREFORE, the Parties mutually agree as follows:

DEFINITIONS

“Administrator” means the Executive Director, Orange County Community Services.

“Allocation” means the process of assigning a cost, or a group of costs, to one or more cost objective(s), in reasonable proportion to the benefit provided or other equitable relationship. The process may entail assigning a cost(s) directly to a final cost objective or through one or more intermediate cost objectives. (2 CFR 200.4 and 45 CFR 75.2)

“County’s Contract Administrator” means the Contract Manager who shall administer this Contract as is necessary or reasonable to comply with County policies.

“Disallowed costs” means those charges determined to be unallowable, in accordance with the applicable Federal statutes, regulations, or the terms and conditions of the Federal award. (2 CFR 200.31 and 200.425 and 45 CFR 75.2)

“DUNS Number:” A unique 9-digit identifier issued and maintained by Dun & Bradstreet (D&B) that verifies the existence of a business entity. The DUNS number is needed to coordinate with the System for Award Management (SAM) that combines federal procurement systems and the Catalog of Federal Domestic Assistance into one new system. <https://www.SAM.gov>.

“Questioned Costs” means a cost that is questioned by the auditor because of an audit finding which resulted from a violation or possible violation of a statute, regulation, or the terms and conditions of a

Federal award, including for funds used to match Federal funds; where the costs, at the time of the audit, are not supported by adequate documentation; or where the costs incurred appear unreasonable and do not reflect the actions a prudent person would take in the circumstances. (2 CFR 200.84, 200.425 and 45 CFR 75.2).

“Recoverable cost” means the state and federal share of the questioned cost.

“Subcontractor” and “subcontractor” means any entity that furnishes to Contractor services or supplies related to this Contract.

ARTICLES

General Terms and Conditions:

- A. **Governing Law and Venue:** This Contract has been negotiated and executed in the State of California and shall be governed by and construed under the laws of the State of California. In the event of any legal action to enforce or interpret this Contract, the sole and exclusive venue shall be a court of competent jurisdiction located in Orange County, California, and the Parties hereto agree to and do hereby submit to the jurisdiction of such court, notwithstanding Code of Civil Procedure Section 394. Furthermore, the Parties specifically agree to waive any and all rights to request that an action be transferred for adjudication to another county.
- B. **Entire Contract:** This Contract contains the entire Contract between the Parties with respect to the matters herein, and there are no restrictions, promises, warranties or undertakings other than those set forth herein or referred to herein. No exceptions, alternatives, substitutes or revisions are valid or binding on County unless authorized by County in writing. Electronic acceptance of any additional terms, conditions or supplemental Contracts by any County employee or agent, including but not limited to installers of software, shall not be valid or binding on County unless accepted in writing by County's Contract Administrator.
- C. **Amendments:** No alteration or variation of the terms of this Contract shall be valid unless made in writing and signed by the Parties; no oral understanding or agreement not incorporated herein shall be binding on either of the Parties; and no exceptions, alternatives, substitutes or revisions are valid or binding on County unless authorized by County in writing.
- D. **Intentionally left blank**
- E. **Delivery:** Time of delivery of goods or services is of the essence in this Contract. County reserves the right to refuse any goods or services and to cancel all or any part of the goods not conforming to applicable specifications, drawings, samples or descriptions or services that do not conform to the prescribed statement of work. Acceptance of any part of the order for goods shall not bind County to accept future shipments nor deprive it of the right to return goods already accepted at Contractor's expense. Over shipments and under shipments of goods shall be only as agreed to in writing by County. Delivery shall not be deemed to be complete until all goods or services have actually been received and accepted in writing by County.
- F. **Acceptance Payment:** Unless otherwise agreed to in writing by County, 1) acceptance shall not be deemed complete unless in writing and until all the goods/services have actually been received, inspected, and tested to the satisfaction of County, and 2) payment shall be made in arrears after satisfactory acceptance.
- G. **Warranty:** Contractor expressly warrants that the services covered by this Contract are fit for the particular purpose for which they are intended. Acceptance of this order shall constitute an agreement upon Contractor's part to indemnify, defend and hold County and County Indemnitees as identified in Paragraph Z below, harmless from liability, loss, damage and expense, including reasonable counsel fees, incurred or sustained by County by reason of the failure of the services to conform to such warranties, faulty work performance, negligent or unlawful acts, and non-compliance with any applicable state or federal codes, ordinances, orders, or statutes, including

the Occupational Safety and Health Act (OSHA) and the California Industrial Safety Act. Such remedies shall be in addition to any other remedies provided by law.

- H. **Patent/Copyright Materials/Proprietary Infringement:** Unless otherwise expressly provided in this Contract, Contractor shall be solely responsible for clearing the right to use any patented or copyrighted materials in the performance of this Contract. Contractor warrants that any software as modified through services provided hereunder will not infringe upon or violate any patent, proprietary right, or trade secret right of any third party. Contractor agrees that, in accordance with the more specific requirement contained in paragraph “Z” below, it shall indemnify, defend and hold County and County Indemnitees harmless from any and all such claims and be responsible for payment of all costs, damages, penalties and expenses related to or arising from such claim(s), including, costs and expenses but not including attorney’s fees.
- I. **Assignment:** The terms, covenants, and conditions contained herein shall apply to and bind the heirs, successors, executors, administrators and assigns of the Parties. Furthermore, neither the performance of this Contract nor any portion thereof may be assigned by Contractor without the express written consent of County. Any attempt by Contractor to assign the performance or any portion thereof of this Contract without the express written consent of County shall be invalid and shall constitute a breach of this Contract.
- J. **Non-Discrimination:** In the performance of this Contract, Contractor agrees that it will comply with the requirements of Section 1735 of the California Labor Code and not engage nor permit any subcontractors to engage in discrimination in employment of persons because of the race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, marital status, or sex of such persons. Contractor acknowledges that a violation of this provision shall subject Contractor to penalties pursuant to Section 1741 of the California Labor Code.
- K. **Termination:** In addition to any other remedies or rights it may have by law, County has the right to immediately terminate this Contract without penalty, cost, expense or liability of any kind for cause or after 30 days’ written notice without cause, unless otherwise specified. Cause shall be defined as any material breach of contract or any misrepresentation or fraud on the part of the Contractor. Exercise by County of its right to terminate the Contract for cause or without cause shall relieve County of all further obligation, cost, expense or liability of any kind.
1. Termination for cause includes, among other things, the County’s termination of the Contract in the event of:
 - i. A violation of the law or failure to comply in a timely manner with any condition of this Contract;
 - ii. Inadequate program performance;
 - iii. Failure to comply with reporting requirements;
 - iv. Evidence that Contractor is in such an unsatisfactory financial condition, as determined by County, as to endanger performance of this Contract, including the loss of other funding sources;
 - v. Delinquency in payment of taxes or the costs of performance of this Contract in the ordinary course of business;

- vi. Appointment of a trustee, receiver or liquidator for all or a substantial part of Contractor's property, or institution of bankruptcy, reorganization, arrangement of liquidation proceedings by or against Contractor;
- vii. Service of any writ of attachment, levy of execution, or commencement of garnishment proceedings against Contractor's assets or income;
- viii. Bankruptcy proceedings of Contractor;
- ix. Finding of debarment or suspension;
- x. Material change in Contractor's organizational structure;
- xi. Any breach of Contract,
- xii. Any misrepresentation, or fraud on the part of the Contractor;

County may terminate this Contract and be relieved of the payment of any compensation to Contractor.

In the event of such termination, County may proceed with the work for which this Contract provides in any manner deemed proper by County. The cost to County of completing the work for which this Contract provides shall be deducted from any sums due Contractor under this Contract but Contractor shall not be relieved of liability. Notwithstanding the above, Contractor shall not be relieved of liability to County for damages sustained by County by virtue of any breach of this Contract by , and County may withhold any payments to Contractor until such time as the exact amount of damages due County from Contractor is determined.

2. Termination for convenience. County may terminate this Contract, without cause, upon thirty (30) days written notice to Contractor, except County may terminate this Contract for failure of any of the funding contingencies set forth in Paragraph BB, Contingency of Funds, upon ten (10) days written notice to Contractor.
3. Return of funds. Contractor agrees that upon expiration or notice of termination of this Contract or dissolution of Contractor's entity, Contractor shall, immediately upon written demand, return to County all funds paid to Contractor by County, which are not payable for goods or services delivered prior to the termination or expiration of this Contract or the dissolution of Contractor's entity.
4. Cancellation of commitments/termination claim. After receipt of notice of termination, Contractor shall cancel outstanding commitments required by this Contract.
 - i. With respect to the above-cancelled commitments, Contractor agrees to provide, within ten (10) days of a notice of termination, a plan for settlement of all outstanding liabilities and all claims arising out of such cancellation of commitments. Such plan shall be subject to the approval of Administrator.
 - ii. Contractor shall submit a termination claim to Administrator promptly after receipt of a notice of termination, but in no event later than sixty (60) days from the effective date thereof unless an extension, in writing, is granted by Administrator.

L. Consent to Breach Not Waiver: No term or provision of this Contract shall be deemed waived and no breach excused, unless such waiver or consent shall be in writing and signed by the party claimed to have waived or consented. Any consent by any party to, or waiver of, a breach by the

other, whether express or implied, shall not constitute consent to, waiver of, or excuse for any other different or subsequent breach.

- M. Independent Contractor:** Contractor shall be considered an independent contractor and neither Contractor, its employees, nor anyone working under Contractor shall be considered an agent or an employee of County. Neither Contractor, its employees nor anyone working under Contractor shall qualify for workers' compensation or other fringe benefits of any kind through County. Contractor will be responsible for any and all tax consequences of receiving grant funds including, but not limited to, issuance of a Form 1099 by the County.
- N. Performance Warranty:** Contractor shall warrant all work under this Contract, taking necessary steps and precautions to perform the work to County's satisfaction. Contractor shall be responsible for the professional quality, technical assurance, timely completion and coordination of all documentation and other goods/services furnished by the Contractor under this Contract. Contractor shall perform all work diligently, carefully, and in a good and workmanlike manner; shall furnish all necessary labor, supervision, machinery, equipment, materials, and supplies, shall at its sole expense obtain and maintain all permits and licenses required by public authorities, including those of County required in its governmental capacity, in connection with performance of the work. If permitted to subcontract, Contractor shall be fully responsible for all work performed by subcontractors.
- O. Insurance Requirements:**
Prior to the provision of services under this Contract, the Contractor agrees to purchase all required insurance at Contractor's expense, including all endorsements required herein, necessary to satisfy the County that the insurance provisions of this Contract have been complied with. Contractor agrees to keep such insurance coverage, Certificates of Insurance, and endorsements on deposit with the County during the entire term of this Contract. In addition, all subcontractors performing work on behalf of Contractor pursuant to this Contract shall obtain insurance subject to the same terms and conditions as set forth herein for Contractor.

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

All self-insured retentions (SIRs) shall be clearly stated on the Certificate of Insurance. Any self-insured retention (SIR) in an amount in excess of Fifty Thousand Dollars (\$50,000) shall specifically be approved by the County's Risk Manager, or designee, upon review of Contractor's current audited financial report. If Contractor's SIR is approved, Contractor, in addition to, and without limitation of, any other indemnity provision(s) in this Contract, agrees to all of the following:

- 1) In addition to the duty to indemnify and hold the County harmless against any and all liability, claim, demand or suit resulting from Contractor's, its agents, employee's or

subcontractor's performance of this Contract, Contractor shall defend the County at its sole cost and expense with counsel approved by Board of supervisors against same; and

- 2) Contractor's duty to defend, as stated above, shall be absolute and irrespective of any duty to indemnify or hold harmless; and
- 3) The provisions of California Civil Code Section 2860 shall apply to any and all actions to which the duty to defend stated above applies, and the Contractor's SIR provision shall be interpreted as though the Contractor was an insurer and the County was the insured.

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

Qualified Insurer

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

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

The policy or policies of insurance maintained by the Contractor shall provide the minimum limits and coverage as set forth below:

<u>Coverage</u>	<u>Minimum Limits</u>
Commercial General Liability	\$1,000,000 per occurrence \$2,000,000 aggregate
Automobile Liability including coverage for owned, non-owned and hired vehicles	\$1,000,000 per occurrence
Workers Compensation	Statutory
Employers Liability Insurance	\$1,000,000 per occurrence
Network Security & Privacy Liability	\$1,000,000 per claims-made
Professional Liability	\$1,000,000 per claims-made \$1,000,000 aggregate
Sexual Misconduct	\$1,000,000 per occurrence
Employee Dishonesty	\$100,000 per occurrence

Technology Errors & Omissions*	\$1,000,000 per claims-made
	\$1,000,000 aggregate

Required Coverage Forms

The Commercial General Liability coverage shall be written on Insurance Services Office (ISO) form CG 00 01, or a substitute form providing liability coverage at least as broad.

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

Required Endorsements

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

- 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, agents and employees*** as Additional Insureds, or provide blanket coverage, which will state ***AS REQUIRED BY WRITTEN Contract.***
- 2) A primary non-contributing endorsement using ISO form CG 20 01 04 13, or a form at least as broad evidencing that the Contractor's insurance is primary and any insurance or self-insurance maintained by the County of Orange shall be excess and non-contributing.

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

- 1) An Additional Insured endorsement naming the ***County of Orange, its elected and appointed officials, officers, agents and employees*** as Additional Insureds for its vicarious liability.
- 2) A primary and non-contributing endorsement evidencing that the Contractor's insurance is primary and any insurance or self-insurance maintained by the County of Orange shall be excess and non-contributing.

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

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

The County of Orange shall be the loss payee on the Employee Dishonesty coverage. A Loss Payee endorsement evidencing that the County of Orange is a Loss Payee shall accompany the Certificate of Insurance.

Contractor shall notify County in writing within thirty (30) days of any policy cancellation and ten (10) days for non-payment of premium and provide a copy of the cancellation notice to

County. Failure to provide written notice of cancellation may constitute a material breach of the Contract, upon which the County may suspend or terminate this Contract.

If Contractor's Professional Liability and Network Security & Privacy Liability are "Claims-Made" policy(ies), Contractor shall agree to maintain coverage for two (2) years following the completion of the Contract.

If Contractor's Professional Liability, Technology Errors & Omissions and/or Network Security & Privacy Liability are "Claims-Made" policy(ies), Contractor shall agree to maintain coverage for two (2) years following the completion of the Contract.

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

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

If the Contractor fails to provide the insurance certificates and endorsements within seven (7) days of notification by the Contract Administrator, award may be made to the next qualified vendor.

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

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

The procuring of such required policy or policies of insurance shall not be construed to limit Contractor's liability hereunder nor to fulfill the indemnification provisions and requirements of this Contract, nor act in any way to reduce the policy coverage and limits available from the insurer.

- P. **Changes:** Contractor shall make no changes in the work or perform any additional work without the County's specific written approval.
- Q. **Change of Ownership/Name, Litigation Status, Conflicts with County Interest:** Contractor agrees that if there is a change or transfer in ownership of Contractor's business prior to completion of this Contract, and the County agrees to an assignment of the Contract, the new owners shall be required under terms of sale or other instruments of transfer to assume Contractor's duties and obligations contained in this Contract and complete them to the satisfaction of the County.

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

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

The Contractor shall exercise reasonable care and diligence to prevent any actions or conditions that could result in a conflict with County interests. In addition to the Contractor, this obligation shall apply to the Contractor's employees, agents, and subcontractors associated with the provision of goods and services provided under this Contract. The Contractor's efforts shall include, but not be limited to establishing rules and procedures preventing its employees, agents, and subcontractors from providing or offering gifts, entertainment, payments, loans or other considerations which could be deemed to influence or appear to influence County staff or elected officers in the performance of their duties.

- R. **Force Majeure:** Contractor shall not be assessed with liquidated damages or unsatisfactory performance penalties during any delay beyond the time named for the performance of this Contract caused by any act of God, war, civil disorder, employment strike or other cause beyond its reasonable control, provided Contractor gives written notice of the cause of the delay to County within 36 hours of the start of the delay and Contractor avails himself of any available remedies.
- S. **Confidentiality:** Contractor shall ensure the confidentiality, protection and preservation of the County's Confidential Information (defined below) and information of a confidential, sensitive, and/or proprietary nature, which may be disclosed or made available to Contractor for its performance of services under this Contract, all related subordinate agreements, and its cyber security assessment and audit of the County's network equipment, and associated software, information and documentation (collectively, the "Purpose").
- a. "Confidential Information" means all non-public information, material, or documents, of any kind obtained from, or on behalf of, the County through any medium that is:
- i. Designated in writing as "confidential" or "private" at the time of its disclosure; or
 - ii. The County's sensitive security information, technical data, programs, software (including configuration or source codes), technical information, screen shots, customer information, employee records, computer network, or architectural or engineering information; or
 - iii. Exploitable data, information protected by privacy law, or other information that is treated as confidential by the County, or is prohibited from being disclosed for any reason pursuant to law, statute, regulation, ordinance, or contract; or

- iv. Any County information security record the disclosure of which would reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of the County; or
- v. Information obtained by Contractor and relating to the County during Contractor's performance of the Contract, any related subordinate agreements, or the Purpose, that a reasonable person knows or reasonably should understand to be confidential and is treated confidential by the disclosing party.
- vi. Information, material or documents that is protected or treated as confidential under a law, rule, or regulation that currently exists or exists at any time during or after the Term of this Contract.

T. Compliance with Laws: Contractor represents and warrants that services to be provided under this Contract shall fully comply, at Contractor's expense, with all standards, laws, statutes, restrictions, ordinances, requirements, and regulations (collectively "laws"), including, but not limited to those issued by County in its governmental capacity, all other laws applicable to the services at the time services are provided to and accepted by County, and the laws set forth in Attachment D (Federal Award Identification Information). Contractor acknowledges that County is relying on Contractor to ensure such compliance, and pursuant to the requirements of paragraph "Z" below, Contractor agrees that it shall defend, indemnify and hold County and County Indemnitees harmless from all liability, damages, costs and expenses arising from or related to a violation of such laws.

U. Intentionally left blank

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

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

X. Interpretation: This Contract has been negotiated at arm's length and between persons sophisticated and knowledgeable in the matters dealt with in this Contract. In addition, each party had been represented by experienced and knowledgeable independent legal counsel of their own choosing or has knowingly declined to seek such counsel despite being encouraged and given the opportunity to do so. Each party further acknowledges that they have not been influenced to any extent whatsoever in executing this Contract by any other party hereto or by any person representing them, or both. Accordingly, any rule or law (including California Civil Code Section 1654) or legal decision that would require interpretation of any ambiguities in this Contract against the party that has drafted it is not applicable and is waived. The provisions of this Contract shall be interpreted in a reasonable manner to affect the purpose of the Parties and this Contract.

Y. Employee Eligibility Verification: The Contractor warrants that it fully complies with all Federal and State statutes and regulations regarding the employment of aliens and others and that all its employees performing work under this Contract meet the citizenship or alien status requirement set forth in Federal statutes and regulations. The Contractor shall obtain, from all employees performing work hereunder, all verification and other documentation of employment

eligibility status required by Federal or State statutes and regulations including, but not limited to, the Immigration Reform and Control Act of 1986, 8 U.S.C. §1324 et seq., as they currently exist and as they may be hereafter amended. The Contractor shall retain all such documentation for all covered employees for the period prescribed by the law. The Contractor shall indemnify, defend with counsel approved in writing by County, and hold harmless, the County, and its County Indemnitees, its agents, officers, and employees from employer sanctions and any other liability which may be assessed against the Contractor or the County or County Indemnitees, any combination of the three in connection with any alleged violation of any Federal or State statutes or regulations pertaining to the eligibility for employment of any persons performing work under this Contract.

Z. Indemnification: Contractor agrees to indemnify, defend with counsel approved in writing by County, and hold County, its elected and appointed officials, officers, employees, agents and those special districts and agencies which County's Board of Supervisors acts as the governing Board ("County Indemnitees") harmless from any claims, demands or liability of any kind or nature, including but not limited to personal injury or property damage, arising from or related to the services, products or other performance provided by Contractor, its agents, employees, affiliates or subcontractors, pursuant to this Contract. If judgment is entered against Contractor and County by a court of competent jurisdiction because of the concurrent active negligence of County or County Indemnitees, Contractor and County agree that liability will be apportioned as determined by the court. Neither party shall request a jury apportionment.

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

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

Contractor agrees to maintain such records for possible audit for a minimum of three (3) years after final payment, unless a longer period of records retention is stipulated under this Contract or by law. Contractor agrees to allow interviews of any employees or others who might reasonably have information related to such records. Further, Contractor agrees to include a similar right to the County to audit records and interview staff of any subcontractor related to performance of this Contract.

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

BB. Contingency of Funds: Contractor acknowledges that funding or portions of funding for this Contract may be contingent upon State or Federal budget approval; receipt of funds from, and/or obligation of funds by, the State of California or Federal government to County; and inclusion of sufficient funding for the services hereunder in the budget approved by County's Board of

Supervisors for each fiscal year covered by this Contract. If such approval, funding or appropriations are not forthcoming, or are otherwise limited, County may terminate upon ten (10) days written notice or modify this Contract without penalty.

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

THE REMAINDER OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Additional Terms and Conditions:

1. **Scope of Contract:** This Contract specifies the contractual terms and conditions by which the County will procure ARPA (H.R. 1319) –Support of Orange County Human Relations Commission from Contractor as further detailed in the Scope of Work, identified and incorporated herein by this reference as Attachment A.
2. **Term of Contract:** This Contract shall commence on December 14, 2022, and continue through June 30, 2024, unless otherwise terminated by the County.
3. **Renewal:** This Contract may be renewed by mutual written agreement of both Parties for two (2) additional one (1) year terms. The County does not have to give reason if it elects not to renew. Renewal periods may be subject to approval by the County of Orange Board of Supervisors. The costs for any renewal periods shall be substantially similar to the initial term of the Contract and continue to be reasonable and necessary for all renewals. In connection with a possible renewal, the County shall have the right to consider Contractor’s actual expenditures, the units of service, the current cost policy standards, and changes in program requirements, and Contractor shall, upon the County’s request, promptly provide to the County all documentation related to such items.
4. **Headings:** The various headings and numbers herein, the grouping of provisions of this Contract into separate clauses and paragraphs, and the organization hereof are for the purpose of convenience only and shall not limit or otherwise affect the meaning hereof.
5. **Maximum Obligation:** The total Maximum Obligation of County to the Contractor for the cost of services provided in accordance with this Contract is \$750,000 as further detailed in the Budget and Staffing Plan, identified and incorporated herein by this reference as Attachment C.
6. **Amendments – Changes/Extra Work:** The Contractor shall make no changes to this Contract without the County’s written consent. In the event that there are new or unforeseen requirements, the County has the discretion with the Contractor’s concurrence, to make changes at any time without changing the scope or price of the Contract.

If County-initiated changes or changes in laws or government regulations affect price, the Contractor’s ability to deliver services, or the project schedule, the Contractor will give County written notice no later than ten (10) days from the date the law or regulation went into effect or the date the change was proposed and Contractor was notified of the change. Such changes shall be agreed to in writing and incorporated into a Contract amendment. Said amendment shall be issued by the County-assigned Contract Administrator, shall require the mutual consent of all Parties, and may be subject to approval by the County Board of supervisors. Nothing herein shall prohibit the Contractor from proceeding with the work as originally set forth or as previously amended in this Contract.

7. **Breach of Contract:** The failure of the Contractor to comply with any of the provisions, covenants or conditions of this Contract shall be a material breach of this Contract. In such event the County may, and in addition to any other remedies available at law, in equity, or otherwise specified in this Contract:
 - a) Terminate the Contract immediately, pursuant to Paragraph K herein;

- b) Afford the Contractor written notice of the breach and ten (10) calendar days or such shorter time that may be specified in this Contract within which to cure the breach;
 - c) Discontinue payment to the Contractor for and during the period in which the Contractor is in breach; and
 - d) Offset against any monies billed by the Contractor but yet unpaid by the County those monies disallowed pursuant to the above.
8. **Conditions Affecting Work:** The Contractor shall be responsible for taking all steps reasonably necessary, to ascertain the nature and location of the work to be performed under this Contract; and to know the general conditions which can affect the work or the cost thereof. Any failure by the Contractor to do so will not relieve Contractor from responsibility for successfully performing the work without additional cost to the County. The County assumes no responsibility for any understanding or representations concerning the nature, location(s) or general conditions made by any of its officers or agents prior to the execution of this Contract, unless such understanding or representations by the County are expressly stated in the Contract.
9. **Conflict of Interest – Contractor’s Personnel:** The Contractor shall exercise reasonable care and diligence to prevent any actions or conditions that could result in a conflict with the best interests of the County. This obligation shall apply to the Contractor; the Contractor’s employees, agents, and subcontractors associated with accomplishing work and services hereunder. The Contractor’s efforts shall include, but not be limited to establishing precautions to prevent its employees, agents, and subcontractors from providing or offering gifts, entertainment, payments, loans or other considerations which could be deemed to influence or appear to influence County staff or elected officers from acting in the best interests of the County.
- The Contractor shall not use moneys provided under this Contract to pay or reimburse any staff person of Contractor or any consultant to Contractor, if such staff person or consultant is a member of the Board of Directors, or other official governing body, of Contractor. Contractor shall further be subject to the full texts of local, State and federal conflict of interest statutes applicable to this Contract.
10. **Conflict of Interest – County Personnel:** The County of Orange Board of Supervisors policy prohibits its employees from engaging in activities involving a conflict of interest. The Contractor shall not, during the period of this Contract, employ any County employee for any purpose.
11. **Service Contract – Follow-On Work:** No person, firm, subsidiary or subcontractor of a firm that has been awarded a consulting services contract or a contract which includes a consulting component may be awarded a Contract for the performance of services, the purchase of goods or supplies, or the provision of any other related action which arises from or can reasonably be deemed an end-product of work performed under the initial consulting to consulting-related Contract.
12. **Project Manager, County:** The County shall appoint a Project Manager to act as liaison between the County and the Contractor during the term of this Contract. The County’s Project Manager shall coordinate the activities of the County staff assigned to work with the Contractor.

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

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

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

A. Copyrights

1. If any material funded by this Contract is subject to copyright, the State of California reserves the right to copyright such material and the Contractor agrees not to copyright such material, except as set forth in Paragraph 14(B) below.
2. The Contractor may request permission to copyright material by writing to the Director of OC Community Services. The OC Community Services will inform Contractor of the decision within approximately sixty (60) days of receipt of the request.
3. If the material is copyrighted with the consent of OC Community Services, the County reserves, and Contractor hereby grants to the County, a royalty-free, non-exclusive, and irrevocable license to reproduce, prepare derivative works, publish, distribute and use such materials, in whole or in part, and to authorize others to do so, provided written credit is given to the author. Contractor also hereby grants to the County, a royalty-free, non-exclusive, and irrevocable license to reproduce, prepare derivative works, publish, distribute and use such materials, in whole or in part, and to authorize others to do so, provided written credit is given to the author.
4. The Contractor certifies that it has appropriate systems and controls in place to ensure that ARPA (H.R. 1319) and/or County funds will not be used in the performance of this Contract for the acquisition, operation, or maintenance of computer software in violation of copyright laws.

B. Rights in Data

1. The Contractor shall not publish or transfer any materials, as defined in Paragraph 14(B)(2) below, produced or resulting from activities supported by this Contract without the express written consent of the Director of OC Community Services. County may request a copy of the material for review prior to approval of the request. This subsection is not intended to prohibit the Contractor from sharing identifying client information authorized by the participant or summary program information which is not client-specific.

2. As used in this Contract, the term “subject data” means writings, sound recordings, pictorial reproductions, drawings, designs or graphic representations, procedural manuals, forms, diagrams, workflow charts, equipment descriptions, data files and data processing or computer programs, and works of any similar nature (whether or not copyrighted or copyrightable) which are first produced or developed under this Contract. The term does not include financial reports, or cost analyses and similar information incidental to contract administration, or the exchange of that information between OC Community Services to facilitate uniformity of contract and program administration on a statewide basis.

15. **Licenses:** At its own expense, Contractor and its subcontractors, if any, shall, at all time during the term of this Contract, maintain in full force and effect such licenses or permits as may be required by the State of California or any other government entity. Contractor and his subcontractors, if any, shall strictly adhere to, and obey, all governmental rules and regulations now in effect or as subsequently enacted or modified, as promulgated by any local, State, or Federal governmental entity.

16. **Disputes – Contract:**

A. The Parties shall deal in good faith and attempt to resolve potential disputes informally. If the dispute concerning a question of fact arising under the terms of this Contract is not disposed of in a reasonable period of time by the Contractor’s Project Manager and the County’s Project Manager, such matter shall be brought to the attention of the Contract Administrator by way of the following process:

1. The Contractor shall submit to the agency/department assigned Contract Administrator a written demand for a final decision regarding the disposition of any dispute between the Parties arising under, related to, or involving this Contract, unless the County, on its own initiative, has already rendered such a final decision.
2. The Contractor’s written demand shall be fully supported by factual information, and, if such demand involves a cost adjustment to the Contract, the Contractor shall include with the demand a written statement signed by a senior official indicating that the demand is made in good faith, that the supporting data are accurate and complete, and that the amount requested accurately reflects the Contract adjustment for which the Contractor believes the County is liable.

B. Pending the final resolution of any dispute arising under, related to, or involving this Contract, the Contractor agrees to diligently proceed with the performance of this

Contract, including the delivery of goods and/or provision of services. The Contractor's failure to diligently proceed shall be considered a material breach of this Contract.

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

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

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

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

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

18. **Errors and Omissions:** All reports, files and other documents prepared and submitted by Contractor shall be complete and shall be carefully checked by the professional(s) identified by Contractor as Project Manager and key personnel attached hereto, prior to submission to the County. Contractor agrees that County review is discretionary and Contractor shall not assume that the County will discover errors and/or omissions. If the County discovers any errors or omissions prior to approving Contractor's reports, files and other written documents, the reports, files or documents will be returned to Contractor for correction. Should the County or others discover errors or omissions in the reports, files or other written documents submitted by the Contractor after County approval thereof, County approval of Contractor's reports, files or documents shall not be used as a defense by Contractor in any action between the County and Contractor, and the reports, files or documents will be returned to Contractor for correction.
19. **Non-Supplantation of Funds:** Contractor shall not supplant any Federal, State, or County funds intended for the purposes of this Contract with any funds made available under this Contract. Contractor shall not claim reimbursement from County for, or apply sums received from County with respect to, that portion of its obligations which have been paid by another source of revenue. Contractor agrees that it shall not use funds received pursuant to this Contract, either directly or indirectly, as a contribution or compensation for the purposes of obtaining Federal, State, or

County funds under any Federal, State, or County program without prior written approval from the County.

20. **Satisfactory Work:** Services rendered hereunder are to be performed to the written satisfaction of County. County's staff will interpret all reports and determine the quality, acceptability and progress of the services rendered.
21. **Access and Records:** County, the State of California and the United States Government and/or their representatives, shall have access, for purposes of monitoring, auditing, and examining, to Contractor's activities, books, documents and papers (including computer records and emails) and to records of Contractor's subcontractors, consultants, contracted employees, bookkeepers, accountants, employees and participants related to this Contract. Contractor shall insert this condition in each Contract between Contractor and a subcontractor that is pursuant to this Contract shall require the subcontractor to agree to this condition. Such departments or representatives shall have the right to make excerpts, transcripts and photocopies of such records and to schedule on site monitoring at their discretion. Monitoring activities also may include, but are not limited to, questioning employees and participants and entering any premises or onto any site in which any of the services or activities funded hereunder are conducted or in which any of the records of Contractor are kept. Contractor shall make available its books, documents, papers, financial records, etc., within three (3) days after receipt of written demand by Director which shall be deemed received upon date of sending. In the event Contractor does not make the above referenced documents available within the County of Orange, California, Contractor agrees to pay all necessary and reasonable expenses incurred by County, or County's designee, in conducting any audit at the location where said records and books of account are maintained.
22. **Signature in Counterparts:** The Parties agree that separate copies of this Contract and/or electronic signatures and handwritten signatures may be signed by each of the Parties, and this Contract will have the same force and effect as if the Original had been signed by all the Parties.
23. **Reports/Meetings:** The Contractor shall develop reports and any other relevant documents necessary to complete the services and requirements as set forth in Attachment A. The County's Project Manager and the Contractor's Project Manager will meet on reasonable notice to discuss the Contractor's performance and progress under this contract. If requested, the Contractor's Project Manager and other project personnel shall attend all meetings. The Contractor shall provide such information that is requested by the County for the purpose of monitoring progress under this contract.
24. **Subcontracting:** No performance of this Contract or any portion thereof may be subcontracted by the Contractor without advance written consent of the County. Any attempt by the Contractor to subcontract any performance of this Contract without the advance written consent of the County shall be invalid and shall constitute a breach of this Contract.

In the event that the Contractor is authorized by the County to subcontract, this Contract shall take precedence over the terms of the Contract between Contractor and subcontractor and shall incorporate by reference the terms of this Contract. The Contractor shall select a subcontractor in accordance to Federal and/or State procurement standards. The County shall look to the Contractor for performance and indemnification and not deal directly with any subcontractor. All work performed by a subcontractor must meet the approval of the County of Orange. Additional Subcontract expectations identified in Attachment A.

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

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

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

26. **Gratuities:** The Contractor warrants that no gratuities, in the form of entertainment, gifts or otherwise, were offered or given by the Contractor or any agent or representative of the Contractor to any officer or employee of the County with a view toward securing the Contract or securing favorable treatment with respect to any determinations concerning the performance of the Contract. For breach or violation of this warranty, the County shall have the right to terminate the Contract, either in whole or in part, and any loss or damage sustained by the County in procuring on the open market any goods or services which the Contractor agreed to supply shall be borne and paid for by the Contractor. The rights and remedies of the County provided in the clause shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Contract.
27. **News/Information Release:** The Contractor agrees that it will not issue any news releases in connection with either the award of this Contract or any subsequent amendment of or effort under this Contract without first obtaining review and written approval of said news releases from the County through the County's Project Manager.
28. **Notices:** Any and all notices, requests, demands and other communications contemplated, called for, permitted, or required to be given hereunder shall be in writing, except through the course of the Parties routine exchange of information and cooperation during the terms of the work and services. Any written communications shall be deemed to have been duly given upon actual in-person delivery, if delivery is by direct hand, or upon delivery on the actual day of receipt or no

greater than four calendar days after being mailed by US certified or registered mail, return receipt requested, postage prepaid, whichever occurs first. The date of mailing shall count as the first day. All communications shall be addressed to the appropriate party at the address stated herein or such other address as the Parties hereto may designate by written notice from time to time in the manner aforesaid.

For County:

OC Community Resources
 OC Community Services
 Project Manager
 1300 S. Grand Ave. Bldg. B, 2nd Floor
 Santa Ana, CA 92705-4407

OC Community Resources
 Contract Development and Management
 Contract Administrator
 601 N. Ross St., 6th Floor
 Santa Ana, CA 92701

For Contractor:

Orange County Human Relations Council
 Alison Edwards, Chief Executive Officer
 1801 E. Edinger Ave., Suite 115
 Santa Ana, CA 92705

29. **Ownership of Documents:** The County has permanent ownership of all directly connected and derivative materials produced under this Contract by the Contractor. All documents, reports and other incidental or derivative work or materials furnished hereunder shall become and remains the sole property of the County and may be used by the County as it may require without additional cost to the County. None of the documents, reports and other incidental or derivative work or furnished materials shall be used by the Contractor without the express written consent of the County. The County shall own, and/or retain ownership of, the Comprehensive Hate Activity Data Tracking & Collection database, all other databases, and all work product produced under this Contract and all intellectual property rights therein.
30. **Precedence:** The Contract documents consist of this Contract and its exhibits and attachments. In the event of a conflict between or among the Contract documents, the order of precedence shall be the provisions of the main body of this Contract, i.e., those provisions set forth in the recitals and articles of this Contract, and then the exhibits and attachments.
31. **Termination – Orderly:** After receipt of a termination notice from the County of Orange, the Contractor may submit to the County a termination claim, if applicable. Such claim shall be submitted promptly, but in no event later than 60 days from the effective date of the termination, unless one or more extensions in writing are granted by the County upon written request of the Contractor. Upon termination County agrees to pay the Contractor for all services performed prior to termination which meet the requirements of the Contract, provided, however, that such compensation combined with previously paid compensation shall not exceed the total compensation set forth in the Contract. Upon termination or other expiration of this Contract, each party shall promptly return to the other party all papers, materials, and other properties of the other held by each for purposes of performance of the Contract.
32. **Default – Re-Procurement Costs:** In case of Contract breach by Contractor, resulting in termination by the County, the County may procure the goods and/or Services from other sources.

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

33. County Branding Requirements:

Publicity, Literature, Advertisement, Social Media, and Avoiding Confusion With County

- A. County owns all rights to the name, logos, and symbols of County. The use and/or reproduction of County's name, logos, or symbols for any purpose, including commercial advertisement, promotional purposes, announcements, displays, or press releases, without County's prior written consent is expressly prohibited.
- B. Contractor may develop and publish information related to this Contract where all of the following conditions are satisfied:
1. Project Manager provides its written approval of the content and publication of the information at least 5 days prior to Contractor publishing the information, unless a different timeframe for approval is agreed upon by the Project Manager;
 2. Unless directed otherwise by Project Manager, the information will include a statement that the program, wholly or in part, is funded through County, State and Federal government funds from the ARPA (H.R. 1319);
 3. All project publicity shall include the following statement: "This project is funded through a grant from the ARPA (H.R. 1319), as allocated by the Orange County Board of Supervisors and administered by OC Community Services."
 4. The information does not give the appearance that the County, its officers, employees, or agencies endorse:
 - a. any commercial product or service; and,
 - b. any product or service provided by Contractor, unless approved in writing by Project Manager; and,
 5. If Contractor uses social media (such as Facebook, Twitter, YouTube or other publicly available social media sites) to publish information related to this Contract, Contractor shall develop social media policies and procedures and have them available to the Project Manager. Contractor shall comply with County Social Media Use Policy and Procedures as they pertain to any social media developed in support of the services described within this Contract. The policy is available on the Internet at <http://www.ocgov.com/gov/ceo/cio/govpolicies>.
- C. Contractor shall use its legal business name (i.e. Orange County Human Relations Council) at all times while performing services under this Contract including, but not limited to, providing community outreach materials and public facing communications. Contractor shall take all necessary steps to avoid the possibility of a likelihood of

confusion between Contractor's programs, trade/entity name, logos, or symbols, and the County's and/or the Orange County Human Relations Commission's programs, names, logos, or symbols. Upon a request by the County, Contractor shall take all measures necessary to achieve the foregoing requirements.

- 34. Policies and Procedures:** Contractor and Contractor's subcontractors, personnel, and all other agents and representatives of Contractor, will at all times comply with and abide by all policies and procedures of County as they now exist or may hereafter be created, changed, modified or amended, that are provided or available to Contractor that reasonably pertain to Contractor in connection with Contractor's performance under this Contract. Such policies include, but are not limited to Attachment E, County Cybersecurity Policy and Attachment F, Certification of Return or Destruction and Non-Data Breach. Contractor shall cooperate with County in ensuring Contractor's compliance with County policies and procedures described in this Contract and as adopted by County from time-to-time, and any material violations or disregard of such policies or procedures shall, in addition to all other available rights and remedies of County, be cause for termination of this Contract.
- 35. Security Policies:** All performance under this Contract shall be in accordance with County's security requirements, policies, and procedures as set forth in this paragraph and in Attachment E, County Cybersecurity Policy, as it now exists or may hereafter be created, amended, modified, supplemented, or replaced by County from time to time, in its sole discretion, by providing Contractor with a written copy of such revised requirements, policies, or procedures (collectively, the "Security Policies"). Contractor shall at all times use industry best practices and methods with regard to the prevention, detection, and elimination, by all appropriate means, of fraud, abuse, and other inappropriate or unauthorized access to County Resources (County systems) and County Data accessed in the performance of Services in this Contract.
- 36. Information Access:** Contractor shall at all times use appropriate safeguard and security measures so as to ensure the confidentiality and security of all County Data. At all times during the term, Contractor shall, and shall cause Contractor personnel and subcontractors, and the employees or agents of any of the foregoing, to fully comply with all of County's policies and procedures regarding data access and security, including those prohibiting or restricting remote access to the County System and County Data, as set forth in the Security Policies. County may require all Contractor personnel performing Services 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 person to whom issued. Contractor shall provide each Contractor person with only such level of access as is required for such individual to perform his or her assigned tasks and functions. From time to time throughout the term, upon request from County but at least once each calendar year, Contractor shall provide County with an accurate, up-to-date list of those Contractor personnel having access to the County System and County Data, and the respective security level or clearance assigned to each such Contractor person. All County Resources (including County systems), and all data contained therein, including County Data, County hardware, and County software used or accessed by Contractor: (a) shall be used and accessed

by such Contractor 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 to access and use the County Systems and County Data, as County in its sole discretion shall deem appropriate.

37. **Data Security Requirements:** Without limiting Contractor's obligation of confidentiality as further described in this Contract, Contractor shall establish, maintain, and enforce a data privacy and information security program, including safety and physical and technical security policies and procedures, to the extent such practices and standards are consistent with and not less protective than the foregoing requirements, are at least equal to applicable best industry practices and standards. Contractor also shall provide technical and organizational safeguards against accidental, unlawful, or unauthorized access to 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, consistent with best industry practice and standards. Further, 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 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 security program prior to commencement of Services and from time to time during the term of this Contract.
38. **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.
39. **General Security Standards:** Contractor will be solely responsible for the information technology infrastructure, including all computers, software, databases, electronic systems (including database management systems) and networks used by or for Contractor to access County Resources (including County systems), County Data or otherwise in connection with the Services ("Contractor Systems") and shall prevent unauthorized access to County Resources (including County systems) or County Data through the Contractor Systems. At all times during

the 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. 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.

40. **Security Failures:** Any failure of the Services 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 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.
41. **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, confidentiality, or integrity of County Data or the physical, technical, administrative, or organizational safeguards put in place by Contractor that relate to the security, confidentiality, or integrity of County Data, Contractor shall, at its own expense, (1) immediately notify the County's Chief Information Security Officer and County Privacy Officer of such occurrence and perform a root cause analysis thereon, (2) investigate such occurrence, (3) provide a remediation plan, acceptable to County, to address the occurrence 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, 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 persons, 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 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 personally identifiable information, 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 and hold County and County Indemnitees harmless from and against any and all claims, including reasonable attorneys fees, costs, and expenses incidental thereto, which may be suffered by, accrued against, charged to, or recoverable from County in connection with the occurrence.

<p>Rafael Linares Chief Information Security Officer 1501 E. St. Andrew Place Santa Ana, CA 92705 Office: (714) 567-7611 E-mail: Rafael.linares@ocit.ocgov.com</p>	<p>Linda Le, CHPC, CHC, CHP County Privacy Officer 1501 E. St. Andrew Place Santa Ana, CA 92705 Office: (714) 834-4082 Email: linda.le@ocit.ocgov.com securityadmin@ocit.ocgov.com</p>
---	--

42. **Security Audits:** Contractor shall maintain complete and accurate records relating to its SOC Type II or equivalent's data protection practices and the security of any of County hosted content, including any backup, disaster recovery, or other policies, practices or procedures. Further, Contractor shall inform County of any security audit or assessment performed on Contractor's operations, information security program, or disaster recovery plan that includes County hosted 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. If Contractor does not perform a SOC Type II or equivalent audit at least once per calendar year, then County may perform or have performed by an independent security expert its own such security audits, which may include penetration and security tests of Contractor Systems and operating environments. All such testing shall ensure all pertinent County security standards as well as any customer agency requirements (e.g., such as federal tax requirements or HIPPA) are in place. 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 security program. In addition, Contractor will provide to County upon request the most recent third-party SOC 2 Type II report. County may also have 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 if County reasonably determines Contractor fails or has failed to meet its obligations under this paragraph.

Program Specific Terms and Conditions:

43. **Debarment:** Contractor shall execute and abide by the Debarment & Suspension Certification, attached hereto as Exhibit 2 and incorporated herein by this reference, and by so doing declares that it is not debarred or suspended or otherwise excluded from or ineligible for participation in Federal/State assistance programs in accordance with 29 C.F.R. Part 98.

44. Lobbying Certification:

- A. Contractor shall execute and abide by the terms of the “Certification Regarding Lobbying,” which is attached hereto as Exhibit 3 and incorporated herein by this reference. Contractor shall complete and immediately forward to the County’s Project Manager the “Disclosure Form to Report Lobbying,” a copy of which is attached hereto as Exhibit 4 and incorporated herein by this reference, if Contractor, or any person, firm or corporation acting on Contractor’s behalf, engaged or engages in lobbying any federal office, employee, elected official or agency with respect to this Contract or funds to be received by Contractor pursuant to this Contract.
- B. Contractor agrees that the funds provided herein shall not be used to promote, directly or indirectly, any political party, political candidate or political activity, except as permitted by law.
- C. Contractor shall be in compliance with the Byrd Anti-Lobbying Amendment (31 U.S.C. 1352 and 29 CFR Part 93).

45. **Fraud:** Contractor shall immediately report to the Project Manager, in writing, all suspected, alleged, or known instances and facts concerning possible fraud, abuse or criminal activity by either Contractor or its Subcontractor(s) under this Contract. Contractor shall inform staff and the general public of how to report fraud, waste or abuse through appropriate postings of incident reporting notice. The County’s Anti-Fraud Program can be accessed through: <http://ocgov.com/gov/risk/programs/antifraud>.

Contractor shall maintain records, documents, or other evidence of fraud and abuse until otherwise notified by County.

46. **Fiscal Appropriations:** This Contract is subject to and contingent upon available local, state, and/or federal funds and applicable budgetary appropriations being approved by the County of Orange Board of Supervisors for each fiscal year during the term of this Contract. If such appropriations are not approved, the Contract will be terminated, without penalty to the County.

47. Fiscal Accountability:

- A. Contractor shall establish and maintain a sound financial management system, based upon generally accepted accounting principles. Contractor’s system shall provide fiscal control and accounting procedures that will include the following:
 - 1. Information pertaining to sub-grant and Contract awards, obligations, unobligated balances, assets, expenditures, and income;

2. Effective internal controls to safeguard assets and assure their proper use;
 3. A comparison of actual expenditures with budgeted amounts for each sub grant and Contract;
 4. Source documentation to support accounting records; and
 5. Proper charging of costs and cost allocation.
- B. Contractor's Records. Contractor's records shall be sufficient to:
1. Permit preparation of required reports;
 2. Permit tracking of funds to a level of expenditure adequate to establish that funds have not been used in violation of the applicable restrictions on the use of such funds; and;
 3. Permit the tracking of any costs incurred (such as stand-in costs) that are otherwise allowable except for funding limitation.
48. **Indirect Costs:** The maximum reimbursement amount allowable for indirect costs is ten percent (10%) of the Contractor's Modified Total Direct Costs (MTDC), excluding in-kind contributions and nonexpendable equipment. Contractors requesting reimbursement for indirect costs shall retain on file an approved indirect cost rate accepted by all federal awarding agencies or an allocation plan documenting the methodology used to determine the indirect costs. Indirect costs exceeding the maximum ten percent (10%) may be budgeted as in-kind for purposes of meeting matching requirements in Title III and VII programs only. Contractor must receive prior approval from federal awarding agency prior to budgeting the excess indirect costs as in-kind.
49. **Dissolution of Entity:** Contractor shall notify County immediately of any intention to discontinue its existence or bring an action for dissolution.
50. **Performance Standards:** Contractor shall comply with and adhere to the performance accountability standards and general program requirements defined in Attachment A and applicable regulations. Should the Performance Requirements defined in the Agreement between the State of California and the County of Orange be changed, County shall have the right to unilaterally modify this Contract to meet such requirements.
- A. Accepted professional standards. The performance of work and Services pursuant to this Contract by Contractor and its subcontractor's, if any, shall conform to accepted professional standards associated with all Services provided under this Contract. Contractor shall resolve all issues regarding the performance of Contractor and its subcontractor's, if any, under this Contract using good administrative practices and sound judgment. Contractor shall be accountable to County for the proper use of funds provided to Contractor pursuant to this Contract and for the performance of all work and Services pursuant to this Contract.

B. Performance of Contractor. Contractor agrees to meet the performance standards listed in Attachment A.

Administrator or Contractor may transfer units of Service from one unit of Service to another unit of Service in Attachment "A" as long as the basic goals and objectives of the program are not altered, and prior written agreement is obtained by Contractor from Administrator. Administrator in its sole discretion may increase units of Service in Attachment A as a result of a contingency cost increase. Administrator in its sole discretion may decrease units of service in Attachment A as a result of a contingency cost decrease.

- i. If Administrator determines that Contractor's failure to provide the required levels of Service poses an immediate risk to the health or safety of the older adult clients who should benefit from Services provided by Contractor, and that the most effective method of protecting the interests of the older adults is to obtain the Services described herein from another source, County may terminate this Contract immediately in accordance with Paragraph K hereof and pursue all available legal remedies for breach of this Contract, including, but not limited to, the return by Contractor of all funds paid by County to Contractor that were not expended in accordance with this Contract.
- ii. If Administrator determines that Contractor's failure to provide the required levels of service poses an immediate risk to the health or safety of the older adults who should benefit from services provided by Contractor, and that the most effective method of protecting the interests of the older adults is to require full performance by Contractor of its duties hereunder, County may seek such injunctive relief against Contractor as is appropriate and pursue all other available legal remedies for breach of this Contract, including, but not limited to, the return by Contractor of all funds paid by County to Contractor that were not expended in accordance with this Contract.
- iii. Administrator may demand, and Contractor shall submit upon demand, a corrective action plan that shall include an analysis of the causes of the problem, specific actions to be taken to correct the problem, and a timetable for each such action. The corrective action plan is to be submitted to Administrator within ten (10) days of the request from County and implemented in the required time frame. If Contractor does not carry out the required corrective action within the designated time frame, County shall have the right, in its sole discretion, to take any, or more than one, of the following actions:
 - a. Terminate this Contract pursuant to Paragraph K hereof;
 - b. Discontinue program support until such time as Contractor complies with the corrective action plan;
 - c. Seek appropriate injunctive relief;
 - d. Collect from Contractor all funds paid by County to Contractor that were not expended in accordance with this Contract;
 - e. Collect from Contractor damages for breach of this Contract;
 - f. Reduce the funding available to or hereunder; or
 - g. Pursue any other available legal or equitable remedy against Contractor.

Within five (5) days of demand therefore, Contractor shall repay to County all funds paid by County to Contractor that were not expended in accordance with this Contract.

C. Reporting requirements

- i. Contractor will be required to submit records, statistical information, financial reports, and program information in electronic or paper format as required by the County of Orange OC Community Services.
- ii. Contractor shall retain all collected data for the periods specified in Paragraph 55 of this Contract. County has the right to review this documentation at any time during normal business hours.
- iii. County reserves the right to withhold payment or to terminate this Contract for nonconformance with data collection and reporting requirements.
- iv. Contractor is required to collect and report program data to OC Community Services, including if applicable, properly registering every client receiving services under this Contract, in compliance with the data reporting system required by OC Community Services.
- v. Data shall be collected by Contractor every time a service is delivered to a registered client. Data shall be reported to OC Community Services monthly, or as designated by Administrator.
- vi. Contractor will also be required to submit to OC Community Services other records, statistical information, financial reports, invoices, and program information in electronic or paper format by the 10th of every month unless otherwise authorized by Administrator.
- vii. If County-provided data collection equipment is provided; Contractor must maintain such equipment in a secure office environment.
- viii. Within 10 days of award of this Contract the Contractor must inform OC Community Services of the designated primary and one back-up staff member who will be responsible for “a” through “e” below. The Contractor must inform the OC Community Services within 72 hours of any changes to this designation. New designee(s) will comply with systems training as designated by OC Community Services.
 - a. Supervising the collection of, or collecting data from this program;
 - b. Compiling collected data and reconciling it to data collected;
 - c. Recording collected data in a format required by OC Community Services, using an application required by OC Community Services, if applicable;
 - d. Distributing forms and reports to the responsible person and collecting completed forms; and
 - e. As required, completing all required OC Community Services forms.
- ix. Failure to comply with any portion of the system requirements as herein described violates the instructions and specifications as required by the County. County reserves the right to withhold payment or to terminate this Contract for nonconformance with data collection and reporting requirements.

51. Payments:

Contractor agrees that any and all funds received under this Contract shall be disbursed on or before June 30, and that any and all funds remaining as of June 30, which have not been disbursed shall be returned by Contractor to County within thirty (30) days of the expiration or earlier termination of the Contract in accordance with Paragraph K of this Contract. No expense of Contractor will be reimbursed by County if incurred after June 30.

Upon the effective date of this Contract, County shall make payment to Contractor in accordance with the following payment schedule:

- A. Monthly Payments: Upon receipt and approval by OC Community Resources – OC Community Services of Contractor’s invoice showing prior month(s) actual expenditures, County shall make monthly reimbursement payments based on Contractor’s invoice so long as the total payments under this Contract do not exceed the Contract maximum obligation.
- B. County Discretion: At the sole discretion of County, payments to Contractor may be made more frequently than monthly, but such payments shall always be in arrears and not in advance of the provision of services by Contractor.
- C. Invoices: Contractor shall provide monthly invoices by the 10th day following the month being reported. If the 10th falls on a weekend or holiday, the invoice/data report is due the next business day. Invoices shall show the most up to date costs chargeable to the program(s) referenced in this Contract and in accordance with the OC Community Resources Contract Reimbursement Policy for documenting Contractor costs, incorporated herein by reference as Exhibit 5. Failure to provide any of the required documentation will cause County to withhold all or a portion of a request for reimbursement, or return the entire reimbursement package to Contractor, until such documentation has been received and approved by the County.

The final, complete and correct, invoice must be received by the County no later than July 10, 2024. Any invoice received by the County after July 10, 2024, may not be paid.

- D. Advance Payment: Notwithstanding Paragraphs 42.A and 42.B above, upon written request and justification of an immediate need based upon cash forecasting from Contractor, County may advance to Contractor a portion of County’s maximum obligation hereunder. The County’s Project Manager shall reduce the amount of monthly payments in the second and third months by an equal amount of any advance payment to recover any outstanding advance or part(s) thereof.

No payments will be authorized if any preceding month’s reports or invoices have not been received. Refer to Attachment B, Payment/Compensation for additional information.

52. **Budget and Staffing Plan**: Contractor agrees that the expenditures of any and all funds under this Contract will be in accordance with the Budget Schedule, a copy of which is attached hereto as Attachment C, and which by this reference is incorporated herein and made a part hereof as if fully set forth.

53. **Modification of Budget and Staffing Plan**: Upon written approval, County shall have the authority to transfer allocated program funds from one category of the overall program Budget

to any other category of the overall Budget. No such transfer may be made without the express prior written approval of County. Contractors will be limited to three (3) adjustments per year. Each modification shall be submitted to the Contract Manager no later than 10 days after the end of the first three quarters as necessary. County initiated adjustments do not count towards the three allowed modification each year.

54. **Annual Audit:** Contractor shall arrange for an independent audit to be performed by a Certified Public Accountant, for funds received from County.

55. **Audit Requirements:**

- A. Maintenance and retention. Contractor shall, at all times during the term of this Contract, maintain complete records (which shall include, but not be limited to, accounting records, grants, Contracts, agreements, letters of agreement, insurance documentation, memoranda and/or letters of understanding and client records) of its activities and expenditures hereunder in a form satisfactory to the State and County. All such records must be maintained and kept available by Contractor as follows:
 - i. Until three (3) years after final payment under this Contract, or until an audit has occurred and an audit resolution has been reached, whichever is later, unless otherwise authorized in writing by County; or
 - ii. For such longer period, if any, as is required by applicable statute, by any other Paragraph or Section of this Contract or by Paragraphs “B” or “C” below, or for such longer period as the State or County deem necessary.
- B. Termination of Contract. If this Contract is completely or partially terminated, the records relating to the work terminated shall be preserved and made available for the same periods as set forth in this Paragraph “A” and “C”.
- C. Litigation, claims, etc. In the event of any litigation, claim, negotiation, audit exception, or other action involving the records, all records relative to such action shall be maintained and kept available until three (3) years after every action has been cleared to the satisfaction of County and so stated in writing to Contractor.
- D. Accounting records. Unless otherwise agreed in writing by Administrator, Contractor shall maintain accounting records to account for all funds received under this Contract. Said records shall be separate from the records for any other funds administered by Contractor and shall be kept in accordance with generally accepted accounting principles and procedures. Said records must contain information pertaining to receipt of funds for the program(s) for which this Contract provides, authorization to expend said funds, obligations, unobligated balances, assets, liabilities, outlays or expenditures, contributions, and third-party revenue. Said accounting records must be supported by source documentation (such as cancelled checks, paid bills, payrolls, time and attendance records, Contract and subcontract award documents, etc.), and adequate source documentation of each transaction shall be maintained relative to the allowability of expenditures under this Contract. If the allowability of expenditures cannot be determined because records or documentation of Contractor are nonexistent or inadequate according

to generally accepted accounting principles and procedures, the expenditures will be questioned in the audit and may be disallowed during the audit resolution process.

- E. Financial reporting requirements. Grant funds shall be identified separately. The County requires Contractor to discretely identify State, federal and local grant funding in the Statement of Revenues and Expenditures. In addition, the amounts reported on the Schedule of Revenue and Expenditures shall be displayed in accordance with the contract term.
- F. Sub-contract provisions. Contractor shall place in all of its sub-contracts, if any, made pursuant to, and/or utilizing funds provided by, this Contract, provisions requiring the subcontractor: (1) to make available to County, State and federal officials all of its records with respect to the sub-contract at any time during normal business hours for the purpose of auditing, examining or making excerpts of such records and auditing all invoices, materials, payrolls, records of personnel and other data relating to all matters covered by the sub-contract; and (2) to retain books, documents, papers, records and other evidence pertinent to the sub-contract for the period of time specified in this Paragraph "A", "B", and "C" above.
- G. Audit.
 - i. If Contractor expends more than \$750,000 in federal funds during the term of this Contract, Contractor shall arrange for an audit to be performed, within one hundred fifty (150) days of the end of Contractor's fiscal year and in accordance with 2 CFR Part 200, Subpart F, "Audit Requirements of States, Local Governments, and Non-Profit Organizations," which is incorporated herein by reference. Furthermore, County retains the authority to require Contractor to submit a similarly prepared audit at Contractor's expense even in instances when Contractor's expenditure is less than \$750,000.
 - ii. Contractor shall take the following actions in connection with such audit:
 - a. Ensure that appropriate corrective action is taken to correct instances of noncompliance with federal laws and regulations. Corrective action shall be taken within six months after County receives Contractor's audit report;
 - b. Adjust its own records as necessitated by the audit;
 - c. Permit independent auditors to have access to its records and financial statements as is necessary for County or Contractor to comply with 2 CFR Part 200, Subpart F;
 - d. Submit two copies of its audit reports to County no later than 30 days after completion of the reports;
 - e. Procure audit services in accordance with 2 CFR Part, 215.40 (OMB Circular A-110) procurement standards and provide maximum opportunity for small and minority audit firms;
 - f. Include in Contract(s) with auditor(s) provisions that the auditor(s) will comply with all applicable audit requirements;

- g. Include in its Contract with independent auditors a clause permitting representatives of County or the State to have access to the work papers of the independent auditors;
 - h. Provide to County, the Bureau of State Audits, and their designated representatives, the right to review and to copy all audit reports and any supporting documentation pertaining to the performance of this Contract, and the option to perform audits and/or additional work as needed;
 - i. Cooperate with and participate in any further audits which may be required by County or the State;
 - j. Ensure that its audit addresses all issues contained in any federal OMB Compliance Supplement that applies to its program;
 - k. Ensure that the audit is performed in accordance with Generally Accepted Government Auditing Standards -2 CFR 200.514 and 45 CFR 75.514, is performed by an independent auditor, and is organization-wide;
- iii. Ensure that the audit is all-inclusive, i.e., it includes an opinion (or disclaimer of opinion) of the financial statements; a report on internal control related to the financial statements and major programs; an opinion (or disclaimer of opinion) on compliance with laws, regulations, and the provisions of contracts; and the schedule of findings and questioned costs in accordance with 2 CFR 200.515 and 45 CFR 75.515; If total funds awarded under this Contract equal or exceed \$10,000, Contractor shall be subject to examination and audit, including interviews of its staff, by the County and State of California for a period of three (3) years after final payment under this Contract.
- H. Final financial statement. Within thirty (30) days after termination of this Contract, Contractor shall submit to Administrator a final financial statement detailing all program expenditures and all income received during the term of this Contract or include such a final financial statement with Contractor's final invoice and substantiating reports.

56. Non-Discrimination and Compliance Provisions:

- A. State laws.
- i. Contractor shall, unless exempted, ensure compliance with the requirements of Cal. Gov. Code §11135 et seq., and 2 CCR § 11140 et seq., which prohibit recipients of state financial assistance from discriminating against persons based on race, national origin, ethnic group identification, religion, age, sex, sexual orientation, color, or disability. [22 CCR § 98323]
 - ii. Contractor's signature affixed hereon shall constitute a certification, under penalty of perjury under the laws of the State of California, that Contractor has, unless exempted, complied with the nondiscrimination program requirements of Government Code Section 12900 (a-f) and Title 2, California Code of Regulations, Section 8103.
 - iii. Contractor shall include the nondiscrimination and compliance provisions of this Paragraph 47 "A" in all sub-contracts to perform work under this Contract.

- B. Title VI of Civil Rights Act. Contractor hereby agrees that it will comply with Title VI of the Civil Rights Act of 1964 [42 USC 2000d; 45 CFR 80](P.L. 88-352) and all requirements imposed by or pursuant to the Regulation of the Department of Health and Human Services (45 CFR Part 80) issued pursuant to that title, to the end that, in accordance with Title VI of the Act and the Regulation, no person in the United States shall, on the ground of race, color, or national origin, be excluded from participation in, be denied the benefits of, or be otherwise subjected to discrimination under any program or activity for which funds are made available under this Contract. Contractor hereby gives assurance that it will immediately take any measures necessary to effectuate this Contract.
- C. Title VII of Civil Rights Act. Contractor shall comply with Title VII of the Civil Rights Act of 1964 (42 U.S.C. 2000), as amended by the Equal Opportunity Act of March 24, 1972 (Public Law No. 92-261), and with all applicable rules, regulations and orders promulgated pursuant thereto, as now in existence or as hereafter amended.
- D. Disability discrimination. Contractor shall comply with Sections 503 and 504 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794), the Americans with Disabilities Act of 1990 (42 U.S.C. 12101 et seq.), and all requirements imposed by the applicable regulations and guidelines issued pursuant to those statutes, including 45 CFR, Part 84.
- E. Failure to comply. If Contractor fails to comply with the requirements of any Sub-Paragraphs of this Paragraph 47 Administrator may withhold payment to Contractor and/or terminate this Contract in accordance with Paragraph K.

57. **Drug Free Workplace:** Contractor shall execute and abide by the Drug Free Workplace Certification attached hereto as Exhibit 1 and incorporated herein by this reference.

58. **UEI and D-U-N-S Numbers and Related Information:** UEI and D-U-N-S Numbers: A unique, non-indicative 12-and 9 digit identifiers issued and maintained by SAM.gov and the Dun & Bradstreet (D&B) that verifies the existence of a business entity. The UEI and D-U-N-S Numbers are needed to coordinate with the System for Award Management (SAM) that combines federal procurement systems and the Catalog of Federal Domestic Assistance into one new system. <https://www.SAM.gov>

The UEI and D-U-N-S Numbers must be provided to County prior to the execution of this Contract. Subrecipient shall ensure all UEI and D-U-N-S information is up to date and the UEI and D-U-N-S Numbers status is "active," prior to execution of this Contract. If County cannot access the Subrecipient's UEI and D-U-N-S information related to this federal sub award on the Federal Funding Accountability and Transparency Act Sub Award Reporting System (SAM.GOV) due to errors in the Subrecipient's data entry for its UEI and D-U-N-S Numbers, the Subrecipient must immediately update the information as required.

If County cannot access the Subrecipient's UEI and D-U-N-S information related to this federal sub award on the Federal Funding Accounting and Transparency Act Sub Award Reporting System (SAM.GOV) due to errors in the Subrecipient's data entry for its UEI and D-U-N-S

Numbers, the Subrecipient must immediately update the information as required.

The County reserves the right to verify and validate any information prior to contract award and during the entire term of the Contract.

59. Modification of Program Components and Service Levels: The Parties hereto agree that those program components and service levels detailed in Attachments A, B, C, and/or D may be modified upon mutual written agreement of the Director and Contractor so long as the total payments under this Contract are not increased and the basic goals and objectives of the program are not altered. Should the Federal Government and/or the State of California modify any program component and/or service level detailed in Attachments A, B, C, and/or D then the County shall have the right to unilaterally modify this Contract to meet such requirements.

- A. County may at any time, by written change order to Contractor, make changes within the general scope of this Contract, including, in the definition of services and tasks to be performed, the manner in which services are performed, the time and place of performance thereof and additional related provisions, and Contract term. Such change orders may be made when necessitated by changes in the Orange County OC Community Services operations or performance, the operations or performance of Contractor, or changes in applicable statutes, regulations or State of California or Federal mandates or directives.

Contractor and County shall make a good faith effort to reach agreement with respect to change orders, which affect the price of services under the Contract. Contractor's protest or failure to agree to the amount of any adjustment to be made as a result of a change order shall be a dispute for which an appeal may be made pursuant to this Contract. Notwithstanding the foregoing, the price of services under this Contract shall not be increased except by written modification of this Contract indicating the new services and price of this Contract if applicable. Until the Parties reach agreement, Contractor shall not be obligated to assume increased performance under the change order beyond the limitation of funds established within this Contract.

- B. Contractor may request changes in the scope of performance or services under this Contract, by submitting a written request to Project Manager describing the request and its impact on the Scope of Services and Budget Schedule. Project Manager will review the request and respond in writing within ten (10) business days. Project Manager's decision whether to approve the request or request Board of Supervisors' approval shall be final. County's Contract Administrator may approve a request that meets all of the following criteria:
- i. It does not materially change the terms of this Contract, and
 - ii. It is supported by adequate consideration to County.

Board of Supervisors' action is necessary to approve a request from Contractor that does not satisfy all of the criteria listed above.

60. **Complaint Resolution Process and Grievance Procedures for Participants:** Intentionally left blank.
61. **Sectarian Activities:** Contractor certifies that this Contract does not aid or advance any religious sect, church or creed for a purpose that is sectarian in nature, nor does it help to support or sustain any school, college, university, hospital or other institution controlled by any religious creed, church, or sectarian denomination.
62. **Policies and Procedures:** Contractor shall monitor its program for compliance with the provisions of this Contract. Contractor shall also comply with all applicable parts of County's Policies and Procedures when applicable.
63. **Sweat-free Code of Conduct:** All Contractors contracting for the procurement or laundering of apparel, garments or corresponding accessories, or the procurement of equipment, materials, or supplies, other than procurement related to a public works contract, declare under penalty of perjury that no apparel, garments or corresponding accessories, equipment, or supplies have been furnished to the Contractor from sources that include sweatshop labor, forced labor, convict labor, indentured labor under penal sanction, abusive forms of child labor or exploitation of children in sweatshop labor. The Contractor further declares under penalty of perjury that they adhere to the Sweat-free Code of Conduct as set forth on the California Department of Industrial Relations website located at www.dir.ca.gov, and Public Contract Code Section 6108.

The Contractor agrees to cooperate fully in providing reasonable access to the Contractor's records, documents, agents or employees, or premises if reasonably required by authorized officials of the State or County, the Department of Industrial Relations, or the Department of Justice to determine the Contractor's compliance with the requirements under this paragraph.

64. **S.W.A.G.:** The Contractor and its Subcontractor/Vendors shall comply with Governor's Executive Order 2-18-2011, which bans expenditures on promotional and marketing items colloquially known as "S.W.A.G." or "Stuff We All Get."
65. **Corporate Status:** All corporate Contractors shall be registered with the California Secretary of State and shall be in good standing, without suspension by the California Secretary of State, Franchise Tax Board, or Internal Revenue service. The corporate Contractor shall maintain the good status standing with the Secretary of State of California throughout the term of this Contract. Any change in corporate status or suspension shall be reported by Contractor immediately in writing to County's Project Manager. If Contractor fails to maintain good standing or has failed to be in good standing at the time of the effective date of this Contract, County, in addition to all remedies available under the law and this Contract, pursuant to Termination provision of this Contract, terminate this Contract for cause.

Contractor, by signing this Contract, does swear under penalty of perjury that no more than one (1) final unappealable finding of contempt of court by a federal court has been issued against Contractor within the immediately preceding two-year period because of Contractor's failure to comply with an order of a federal court which orders the Contractor to comply with an order of the National Labor Relations Board.

66. Compliance with Other Laws:

- A. Laws related to Contract. Contractor and its subcontractors shall administer the program(s) funded by this Contract in accordance with this Contract, and with all applicable local, State and federal laws, regulations, directives, guidelines and/or manuals.
- B. Laws applicable to Contractor's operations. Contractor and its subcontractors shall comply with all federal, State and local laws and regulations pertinent to their operations, including, but not limited to all statutes, ordinances, regulations, directives, guidelines and/or manuals pertaining to wages and hours of employment, occupational safety, fire safety, health and sanitation.
- C. Federal environmental laws. If the amount of compensation Contractor shall receive under this Contract exceeds \$100,000, Contractor and its subcontractors shall comply with all applicable orders or requirements issued under the following laws:
- i. Clean Air Act as amended (42 U.S.C. 7401)
 - ii. Federal Water Pollution Control Act as amended (33 U.S.C. 1251 et seq.)
 - iii. Environmental Protection Agency Regulations (40 CFR 29, Executive Order 11738).
 - iv. State Contract Act [Cal. Pub. Con. Code §10295 et seq.]
 - v. Unruh Civil Rights Act [Cal. Pub. Con. Code § 2010]
- D. State Energy Plan. Contractor shall comply with all mandatory standards and policies relating to energy efficiency which are contained in the State Energy Plan issued in compliance with the Energy Policy and Conservation Act (Pub. L. 94-163, 89 Stats. 871).
- E. Withholding. Contractor shall promptly forward payroll taxes, insurances and contributions, including State Disability Insurance, Unemployment Insurance, Old Age Survivors Disability Insurance, and federal and State income taxes withheld, to designated governmental agencies as required by law.
- F. Debarment.
- i. Contractor shall not make any award or permit any award at any time to any party which is debarred or suspended or is otherwise excluded from or ineligible for participation in federal/State assistance programs.
 - ii. Contractor shall timely execute any and all amendments to this Contract or certificates or other required documentation relating to its subcontractors' debarment/suspension status.
- G. State and local environmental and land use laws.
- i. Contractor shall comply with the California Environmental Quality Act (CEQA) and Section 65402 of the Government Code, as may be required by the land use agency of jurisdiction. Contractor further agrees to provide Administrator proof that Contractor has complied with, and maintains compliance with, all zoning regulations and that Contractor has obtained, and is maintaining in full force and effect, all necessary licenses, permits, certifications, and authorizations to operate said programs at each location, or as may otherwise be approved by Administrator.

- ii. By signing this Contract, Contractor swears under penalty of perjury that Contractor is not:
 - a. in violation of any order or resolution not subject to review promulgated by the State Air Resources Board or an air pollution control district;
 - b. subject to cease and desist order not subject to review issued pursuant to Section 13301 of the Water Code for violation of waste discharge requirements or discharge prohibitions; or
 - c. finally determined to be in violation of provisions of federal law relating to air or water pollution.

H. Failure to comply. If Contractor fails to comply with the requirements of any Sections of this Paragraph 57, Administrator may withhold payment to Contractor and/or terminate this Contract in accordance with Paragraph K.

67. **Focal Points:** Intentionally left blank.

68. **Covenant Against Contingent Fees:**

1. The Contractor warrants that no person or selling agency has been employed or retained to solicit this Contract. There has been no agreement to make commission payments in order to obtain this Contract.
2. For breach or violation of this warranty, the County shall have the right to terminate this Contract without liability or at its discretion to deduct from the Contract price or consideration, or otherwise recover, the full amount of such commission, percentage, brokerage, or contingency fee.

THE REMAINDER OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Signature Page

IN WITNESS WHEREOF, the Parties hereto certify that they have read and understand all the terms and conditions contained herein and have hereby caused this Contract to be executed.

***ORANGE COUNTY HUMAN RELATIONS COUNCIL**

By:  _____ By: _____
E72E8BDFED364C7...

Name: Alison Edwards _____ Name: _____

Title: CEO _____ Title: _____

Dated: 11/10/2022 _____ Dated: _____

*For Contractors that are corporations, signature requirements are as follows: 1) One signature by the Chairman of the Board, the President or any Vice President; and 2) One signature by the secretary, any Assistant secretary, the Chief Financial Officer or an Assistant Treasurer.


For Contractors that are not corporations, the person who has authority to bind the Contractor to a contract, must sign on one of the lines above.

COUNTY OF ORANGE
A Political Subdivision of the State of California
COUNTY AUTHORIZED SIGNATURE:

Print Name Title

Signature Dated

APPROVED AS TO FORM
DEPUTY COUNTY COUNSEL

By:  _____ Dated: 11/14/2022 _____
74000D32FE65457
Deputy County Counsel

Support of Orange County Human Relations Programs and Services

Scope of Work

The Commission is an official governmental 11-member commission founded in 1971, whose mission is to handle intergroup tensions; foster mutual understanding among all residents of the County of Orange; and promote measures to eliminate prejudice, intolerance and discrimination against any individual or group. The role of the Commission is to receive and hear specific complaints and problems of discriminations, discuss each matter as appropriate, and when appropriate, make findings and report those findings. The Commission will also engage in research and education for the purpose of lessening and eliminating prejudice and its effects, coordinate and promote educational programs which will foster understanding among various groups within the County, and work for the development of constructive community educational programs to prevent future problems. In addition, the Commission will provide assistance and referral services to individuals and groups, which will facilitate understanding and participation in the decision-making process of County institutions. The actions of the Commission are reported in monthly meeting reports and provided to the County.

A. Program Objectives and Services

Contractor shall provide services at its own facility or at the County, as necessary to perform the requirements of this Contract.

Contractor shall only observe holidays consistent with the County observed holidays.

Contractor shall provide the following Countywide Commission programs, services, and resources, among others:

1. Comprehensive Hate Activity Reporting.

Requirements:

- a. Utilize comprehensive client system tool to report hate activity, available 24/7/365 by phone, text and email to report hate activity.
- b. Language offerings to report hate activity shall be made available through direct links to the top seven (7) threshold languages in the County as identified by the United States Census Bureau. Language translation services may be required for additional languages and dialects and may be provided through an interpretation service (i.e., Google Translate).

Reporting and Performance:

Attachment A

Contractor shall provide the following information, on a monthly basis, to the County in a format to be approved by the County Program Manager:

- Number of calls received, by source (victims, law enforcement, third parties);
- Average wait time before reaching a live voice;
- Number of calls that waited longer than two (2) minutes;
- Average length of call;
- Average response time for callbacks;
- Number of referrals made and to which entity;
- Number of dropped calls;
- Number of calls taken by each agent on a daily, weekly, and monthly basis;
- Breakdown of translations services used; and
- Number of trainings completed to Contact Center staff.

2. Comprehensive Hate Activity Data Tracking & Collection.

Requirements:

- a. Utilize comprehensive, unduplicated, fully automated Hate Activity database with the ability to add case notes tied to a client record; identify client referrals and other resources.
- b. Comprehensive reporting shall include, but not be limited to, the following: features, production of data report, data dashboard and geo-mapping.

Reporting and Performance:

Contractor shall provide the following information, on a monthly basis, to the County in a format to be approved by the County Program Manager:

- Number of self-reported entries input into database;
- Number of community organizations accessing database;
- Number of direct referral sources;
- Breakdown of languages utilized;
- Average response time to self-reported entries;
- Breakdown of client demographics; and
- Breakdown of perpetrator information.

3. Commission Outreach and Education.

Requirements:

- a. Coordinate and deliver multilingual, multicultural, and diverse community outreach, public education, and community initiatives to expand Hate Activity prevention efforts.

Attachment A

- b. Facilitate work groups to build trust and solidarity among Orange County communities.
- c. Build mutual understanding among diverse communities through program such as Outreach Sessions, Community Forums and intergroup and interfaith collaboration.
- d. Teach intergroup respect, collaboration, conflict resolution, reconciliation to youth and adults.

4. Annual Hate Crime Report & Release Event.

Requirements:

- a. Organize, draft, and publish an Orange County Annual Hate Crime Report for submission to the County. Report shall be drafted using Hate Activity data collected during the previous year. At a minimum, the report shall be high structured and in all prescribed manner including a cover page, letter from the Commission Chair, table of contents, include illustrations, a glossary, and specific sections based on data collected.
 - b. Plan and organize and host a Release Event of the Annual Orange County Hate Crime Report for the community at large.
 - c. Organize and lead meetings for the Hate Crime Ad Hoc Committee.
5. Staff Support to the Commission and other administrative services which include, but are not limited, to the following:
- a. Resolving conflict with special skills in intergroup and multi-lingual mediation.
 - b. Promoting the full participation of all people in the decision-making processes of the institutions which affect their lives.
 - c. Conducting activities to eliminate prejudice, intolerance, and discrimination.
 - d. Promoting police community relations through a Police Community Reconciliation Program and various other programs, such as Hate Crime Collaboration, Diverse Community Relations Facilitation, and consulting on contentious human relations issues.
 - e. Supporting Commission meetings, including but not limited to, drafting meeting agendas, coordination of presentations, ensuring Commission meetings are coordinated in accordance with the Ralph M. Brown Act and in compliance with the Commission Bylaws.
 - f. Create relationships with diverse communities and police, so there are paths of communication in place when and if controversial, divisive disputes and issues arise.
 - g. Serve on advisory committees for local city police departments, as well as assist the Orange County Sheriff's Department, to convene a countywide Interfaith Advisory Council.
 - h. Provide community outreach and relationship building throughout the

Attachment A

- County to a broad cross-section of diverse communities.
- i. Organize Police/Diverse Community dialogues in collaboration with the Orange County Sheriff's Department, other police departments and a variety of community and faith-based organizations.
 - j. Assist hate crime victims to reduce their isolation and connect them with resources.
 - k. Conduct speeches, presentations, collaborations and outreach efforts to diverse communities.
 - l. Assist communities with strategies to promote positive intergroup relations, respect for differences, and unity in the face of fear.
 - m. Engage local students, teachers, administrators and parents in outreach programs.
 - n. Comprehensive Hate Activity database data reporting, including but not limited to, number of self-reported entries input into the database, number of community organizations accessing database, number of direct referral sources, breakdown of languages utilized, average response time to self-reported entries, and breakdown of client demographics.
 - o. Comprehensive Client Hate Activity Reporting, including but not limited to, number of calls received by source, average wait time before reaching a live voice, number of calls that waited longer than 2 minutes, average length of call, average response time for callbacks, number of referrals made and to which entity, number of dropped calls, number of calls taken by each agent on a daily, weekly, and monthly basis, breakdown of translation services used, and breakdown of how reporting was completed (phone, text, email).

18-month Activity Matrix December 14, 2022, through June 30, 2024

Activity Requirement	12/14/22 – 3/31/23	4/1/23 – 6/30/23	7/1/23 – 9/30/23	10/1/23 – 12/31/23	1/1/24 – 3/31/24	4/1/24 - 6/30/24	TOTAL
A. Organize meetings for the Hate Crime Prevention Network group and lead hate prevention efforts.	1	1	1	1	1	1	6
B. Monitor and offer support when intergroup relations or bias related community conflicts, tension or crisis arise.	2	2	2	2	2	2	12
C. Follow-up on hate activity reports referred from 211-OC.	3	3	3	3	3	3	18

Attachment A

D. Offer listening sessions or restorative community dialogues process to promote respect and understanding to diverse communities and/or to address tension, conflict, or crisis when it arises (i.e., law enforcement, schools, religious institutions, nonprofits, etc.)	1	1	1	1	1	1	6
E. Service on advisory committees for local city police departments, as well as assist the Orange County Sherriff's Department, to convene a countywide interfaith Advisory Council.	2	2	2	2	2	2	12
F. Deliver multilingual, multicultural, & diverse community-based hate prevention through community outreach, relationship building efforts, collaboration and network meetings, and attending diverse community/law enforcement events	25	25	25	25	25	25	150
G. Provide monthly comprehensive Hate Activity Database & Reporting data reports	3	3	3	3	3	3	18

B. Eligible Populations

Assistance, services and resources shall be available to all residents, communities, cultures, businesses, students, employees, visitors, and volunteers in Orange County, California.



PAYMENT/COMPENSATION

1. COMPENSATION:

This is a cost reimbursement Contract between the County and the Contractor for **\$750,000** in American Rescue Plan Act funding as set forth in Attachment A. Scope of Services attached hereto and incorporated herein by reference. The Contractor agrees to accept the specified compensation as set forth in this Contract as full remuneration for performing all services and furnishing all staffing and materials required, for any reasonably unforeseen difficulties which may arise or be encountered in the execution of the services until acceptance, for risks connected with the services, and for performance by the Contractor of all its duties and obligations hereunder. The County shall have no obligation to pay any sum in excess of the total Contract amount specified unless authorized by an amendment in accordance with paragraphs C and P of the County's General Terms and Conditions.

2. FIRM DISCOUNT AND PRICING STRUCTURE:

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

3. PAYMENT TERMS:

An invoice for services/activities shall be submitted to the address specified below upon the completion of the services/activities and approval of the County Project Manager. Contractor shall reference Contract number on invoice. Payment will be net 30 days after receipt of an invoice in a format acceptable to the County of Orange and verified and approved by OC Community Services and subject to routine processing requirements of the County. The responsibility for providing an acceptable invoice rests with the Contractor.

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

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

Invoice(s) are to be sent to:

OC Community Resources
Auditor Controller / OCCR Accounting
601 N. Ross St., 6th floor
Santa Ana, CA 92701
Attention: Accounts Payable

4. **INVOICING INSTRUCTIONS:**

Further instructions regarding invoicing/reimbursement as set forth in Exhibit 5 OC Community Resources Contract Reimbursement Policy, are attached hereto and incorporated herein by reference.

The Contractor will provide an invoice on Contractor's letterhead for services rendered. Each invoice will have a number and will include the following information:

The Demand Letter/Invoice must include Delivery Order (DO) Number, Contract Number, Service date(s) – Month of Service along with other required documentation (See Exhibit 5).

5. **OC COMMUNITY RESOURCES CONTRACT REIMBURSEMENT POLICY:**

Further instructions regarding invoicing/reimbursements as set forth in Exhibit 5 OC Community Resources Contract Reimbursement Policy, are attached hereto and incorporated herein by reference.



BUDGET AND STAFFING PLAN

Support of OC Human Relations Commission Programs and Services

Budget (December 14, 2022 – June 30, 2024)

Program requirements detailed in Attachment A.

Administrative Cost:	
Personnel (Salaries & Benefits)	\$527,165.00
Administrative Costs (Bookkeeper)	\$9,787.00
Facility Lease	\$8,604.00
Subcontractors:	
211 OC Subcontract: Database & Call Center/Resource Helpline	\$204,444.00
TOTAL	\$750,000

STAFFING PLAN

FTE*

Commission Executive Director	1.00
Sr. Human Relations Specialist	1.00
Sr. Human Relations Specialist	1.00
Sr. Administrative Liaison	0.75
Bookkeeper	0.10

GRAND TOTAL: 3.85

*1.00 FTE = Full-Time Equivalent

Contractor may request to shift funds between budgeted line items for the purpose of meeting specific program needs by utilizing a Budget/Staffing Modification Request form provided by Contract Administrator. Contractor must include a justification narrative specifying the purpose of the request, the amount of said funds to be shifted, and the sustaining annual impact of the shift as may be applicable to the current Fiscal Year Budget and/or future Fiscal Year Budgets. Contractor shall obtain written approval of any Budget/Staffing Modification Request(s) from Contract Administrator prior to implementation by Contractor.

FEDERAL AWARD IDENTIFICATION INFORMATION

The General Program Requirements were designed to provide the framework where the Subrecipient will provide American Rescue Plan Act identified in this attachment.

I. **GOVERNANCE**

The Subrecipient agrees to comply, remain informed, and deliver services consistent with the provisions of the American Rescue Plan Act (“ARPA”) Section 9901 under the Social Security Act Sections 602 and 603.

<https://home.treasury.gov/system/files/136/FRF-Interim-Final-Rule.pdf>

Where local policy has not been set, the Subrecipient agrees to adhere to state and/or federal policy, as appropriate.

II. **GOVERNANCE REFERENCES**

- Additional state and federal agencies that provide funding to the County of Orange/OC Community Resources may be incorporated herein.
- Information Bulletins, Directives, and any other federal and state guidance documents pertaining to the ARPA Funds.
- Actions, directives, and policy and procedures issued by the County of Orange/OC Community Resources.
- County policies, as applicable.

III. **CONTRACTOR/SUBRECIPIENT DETERMINATION:**

In accordance with the requirements of 2 CFR 200.330 (Subrecipient and Contractor determination) and for the purpose of this Contract, Orange County Human Relations Council is determined to be a Subrecipient.

IV. FEDERAL AWARD IDENTIFICATION NUMBER

FAIN INFORMATION		
A.	CONTRACTOR Name:	Orange County Human Relations Council
B.	SAM Unique Entity ID	TFLRQY5PNT89
C.	Federal Award Identification Number (FAIN):	SLFRP1607
D.	Federal Award Date:	March 11, 2021
E.	Subaward Period of Performance:	December 14, 2022- June 30, 2024
F.	Total Amount of Federal Funds Obligated by the Action:	\$372,000
G.	Total Amount of Federal Funds Obligated to the CONTRACTOR:	\$372,000
H.	Total Amount of the Federal Award:	\$616,840,943
I.	Federal Award Project Description:	American Rescue Plan Act
J.	Federal Awarding Agency:	U.S. Department of the Treasury
K.	Name of PTE:	State of California
L.	Contact Information for the Awarding Official:	Dylan Wright, Executive Director
	Phone Number:	(714) 480-2788
	E-mail Address:	Dylan.Wright@occr.ocgov.com
M.	CFDA Number:	21.027
	CFDA Name:	Coronavirus State and Local Fiscal Recovery Funds
N.	Whether Award is R&D:	No
O.	Indirect Cost Rate for the Federal Award:	N/A



County of Orange

County Policy

Subject:	County Cybersecurity Policy (formerly IT Security Policy)
Authority:	County Executive Office: Signature <u><i>Frank Kim</i></u> <small>Digitally signed by Frank Kim DN: cn=Frank Kim, o=County of Orange, ou=CEO, email=frank.kim@ocgov.com, c=US date=2021.05.10.19:35:52-0700</small>
Policy Owner:	CEO-Chief Information Officer: Signature <u><i>Jeel Desai</i></u>
Approval Date:	2/25/2020
Revision Date(s):	5/10/2021
Version No.:	2.0
Policy No.:	0800-12

INTRODUCTION

Information Technology (IT) is a critical component of all primary County business processes. The County's visibility on the Internet, increased use of electronic communication, and dependence on IT resources requires the development, maintenance, and dissemination of a set of common cybersecurity policies designed to protect these assets.

Security threats, such as identity theft, ransomware, and phishing, have been increasing both in frequency and in complexity. Due to these increasing security threats, a common set of safeguards is required to minimize the risk, cost, and duration of any level of disruption to the County's business processes in the event of damage, failure, loss, corruption, or discontinuation of a strategic component of its critical IT infrastructure. Ensuring such an environment requires an enterprise approach to security that does the following:

- Promotes an enterprise view among all County departments.
- Recognizes an interdependent relationship among County departments.
- Requires adherence to a common, minimum security architecture as well as common, minimum related standards, guidelines, and procedures.

Effective cybersecurity is a civic responsibility and requires a team effort involving the participation and support of every County department, employee, and affiliate that deals with information or information systems.

It is the responsibility of every County employee and affiliate to know, understand, and adhere to the policy, procedures, standards, and guidelines contained herein and to conduct their activities accordingly. This policy document has been adopted in order to provide guidance and protection to County employees and to safeguard the information resources entrusted to those employees. Cybersecurity policies raise user awareness of the potential risks associated with IT. Employee awareness through dissemination of policy helps minimize the cost of cybersecurity incidents; accelerate the development of new application systems; and assure the consistent implementation of cybersecurity controls throughout the organization.

The County's Cybersecurity Policy is based upon NIST SP 800-53 standards, and best practices. This Policy is designed to comply with applicable laws and regulations; however, if there is a conflict, applicable laws and regulations shall take precedence. This Policy is to be considered the minimum requirements for providing a secure environment for the development, implementation, and support of IT. Departments shall develop detailed policies and procedures to handle department-specific cases.

The County Cybersecurity Policy and any other standards established under the authority described herein are resources intended to assist County departments to more effectively manage and implement cybersecurity for their IT resources.

Table of Contents

Introduction ii

1 Policy 1

2 Purpose 1

3 Authority 1

4 Scope 1

5 IT Governance Model 2

6 Roles & Responsibilities 3

7 County Cybersecurity Program 8

8 Asset Management 10

9 Controls Management 13

10 Configuration & Change Management 24

11 Vulnerability Management 26

12 cybersecurity Incident Management 27

13 Service Continuity Management 29

14 Risk Management 32

15 External Dependencies Management 34

16 Training & Awareness 36

17 Situational Awareness 37

18 Definitions 39

19 References 40

Appendix A: department listing 41

Appendix B: Facility Listing 42

Appendix C: Device type listing 43

Appendix D: Policy Statement CroSs references 44

Appendix E: Legislative Policy Drivers 51

Appendix F: Employee Acknowledgement 52

1 POLICY

Departments shall develop, implement, and maintain a Cybersecurity Program that consists of policies, procedures, plans, and guidelines for safeguards to protect information during storage, use or in transit.

2 PURPOSE

This document defines County policy to establish a secure environment that safeguards the confidentiality, integrity and availability of the data and information systems used to manage the services provided by the County. **This document is intended to provide minimum standards for departments to use in developing, implementing and maintaining their Cybersecurity Programs.**

2.1 HIPAA

The County Health Insurance Portability and Accountability Act (HIPAA) Policies and the County Cybersecurity Policy address similar topics; however, they function as separate policies. The County Cybersecurity Policy is more comprehensive in scope as compared with the HIPAA Policy. The HIPAA Policy establishes County policy pursuant to federal HIPAA security requirements for use of electronic protected health information (ePHI) by the County and designated health care entities.

ePHI is addressed within both the County Cybersecurity Policy and HIPAA Policy. If a conflict exists between this Policy and the HIPAA Policy, the HIPAA Policy shall prevail.

3 AUTHORITY

The authority to approve information technology (IT) policy for the County is defined in the *Countywide Information Technology Governance policy*.

“The IT Executive Council:

- Is chaired by the CEO
- Reviews and approves new IT projects in excess of \$150,000 a year in all County departments, regardless of funding source presented by the IRC Chair/designee
- Reviews and approves countywide IT:
 - Priorities
 - Strategies
 - Policies
- Ensures that IT priorities:
 - Align with County business goals
 - Are addressed in a cost-effective manner
- Serves as an escalation point for other IT governance groups“

The IT Governance Model, discussed below, includes application/program/product-specific steering committees which may submit Countywide IT policy for approval. This County Cybersecurity Policy was developed and submitted from the Cybersecurity Joint Task Force (CSJTF).

4 SCOPE

This policy applies to all departments in the County as well as all employees, contractors, vendors, customers, and others who utilize, possess or have access to County IT resources.

The policy is applicable to production-level systems. Internal test and experimental systems not connected to a production network do not require the same level of security unless they make use of confidential information or are connected to a system which contains confidential information.

Application development systems may also be exempt provided they are on a network that is physically separated or suitably isolated from production networks. However, if development or test systems are on the same physical or virtual network as production systems or contain confidential information, they shall follow the same security policy as that required of production systems.

This Policy supersedes all prior countywide cybersecurity policies. This document provides a comprehensive Cybersecurity Policy for County departments.

This Policy is designed to comply with applicable laws and regulations; however, if there is a conflict, applicable laws and regulations shall take precedence.

4.1 COMPLIANCE MEASUREMENT

The County shall verify compliance with this Policy.

4.2 VARIANCES

Variations to this Policy shall be documented and approved following the *County Variance Review and Approval Process*.

4.3 NON-COMPLIANCE

Non-compliance with this Policy may result in significant delays to the implementation of information systems and/or technologies. Devices not in compliance with this Policy may have their access to the County's network restricted.

4.4 POLICY CONTROL AND MAINTENANCE

The County Chief Information Security Officer (CISO) is responsible for maintaining this Policy. The County Executive Officer (CEO) shall approve any modifications to this Policy or related procedures. This Policy shall be reviewed at least annually, and any revisions approved by the CEO. Questions regarding this Policy shall be directed to the CISO.

The following groups shall be notified via email and/or in writing upon approval of the policy and upon any subsequent revisions or amendments made to the original document:

- Board of Supervisors
- CEO,
- Department Heads,
- CIO,
- CSJTF, and
- Internal Audit.

5 IT GOVERNANCE MODEL

IT governance consists of leadership, stakeholder engagement, and collaboration processes that ensure that the County's IT investments support overall business strategies and policy objectives. IT governance facilitates general agreement on IT policies, resources, and architecture.

The IT Executive Council receives input from multiple committees, task forces, and working groups, including the CSJTF. Changes or updates to this policy may be proposed by any group. The CSJTF is responsible for researching and proposing IT guiding principles, standards,

policies, and guidelines to the IT Executive Council. The CSJTF makes recommendations to the IT Executive Council through the governance process. As needed, proposals shall be forwarded to the IT Executive Council for review and approval.

6 ROLES & RESPONSIBILITIES

The roles and responsibilities associated with implementation of the County Cybersecurity Policy include:

6.1 COUNTY EXECUTIVE OFFICER

- The County Executive Officer (CEO) approves the County Cybersecurity Policy.

6.2 CHIEF INFORMATION OFFICER

- The Chief Information Officer (CIO) is overall responsible for the County data while it resides or flows on the County enterprise network.
- The CIO is the primary point of contact for the CEO and Board of Supervisors for information technology and cybersecurity.

6.3 CHIEF INFORMATION SECURITY OFFICER

- The Chief Information Security Officer (CISO) is overall responsible for the County's Cybersecurity Program.
- Oversees the creation, implementation, management and enforcement of the County Cybersecurity Program and cybersecurity policies, standards, and procedures.
- Coordinates with departments that regular cybersecurity assessments are performed.
- Assists departments with becoming and/or maintaining compliance with the requirements of applicable federal, state and local laws and regulations.
- Conducts periodic review of Departmental Cybersecurity Programs and provides feedback for the sustainment and/or improvement of cybersecurity plans, policies, standards, and procedures.
- Reports to the CIO on all cybersecurity and privacy activities, and reports to CEO as necessary.

6.4 DEPARTMENT HEADS

- The Department Heads are responsible for determining the acceptable level of risk, as it pertains to the impact of cybersecurity on their respective department's lines of business including approval of Cybersecurity Policy Exemption Request forms (may **NOT** be delegated).
- The Department Heads may appoint, in writing, a member of their staff to function and carry out the duties of the Departmental Information Security Officer (DISO) and Custodian of Records.
- Overall responsible for the integrity of department computer infrastructure and systems
- Overall responsible for application of technical safeguards of department computer infrastructure and systems except those departments participating in OC IT Shared Services.

6.5 OCIT SHARED SERVICES

- Oversees information technology services for departments subscribed to the IT shared services.

- Coordinates with departments (subscribed to IT shared services) the delivery of information technology related initiatives and operational issues.
- Responsible for operation and maintenance of department computer infrastructure and systems for participating departments.
- Responsible for application of technical safeguards of department computer infrastructure and systems for participating departments.

6.6 DEPARTMENT INFORMATION TECHNOLOGY MANAGER

OCIT for shared services agencies

- The Department Information Technology Manager (IT Manager) is directly responsible for all Department Information Systems.
- IT Manager is responsible for ensuring that department IT activities are in compliance with this Policy.

6.7 DEPARTMENT INFORMATION SECURITY OFFICER

- The Department Information Security Officer (DISO) role is authorized by the Department Head and the following functions may be performed:

For departments using Shared Services:

- **Serves as liaison** between CISO, County Privacy Officer and Department for issues pertaining to cybersecurity and privacy.
- **Serves as liaison** between CISO, OCIT technical staff, and the Department for implementation of technical controls and remediation of technical findings from cybersecurity assessments, audits, and cybersecurity incidents.
- **Serves as liaison** between CISO, County Privacy Officer, and Department to annually review and approve the Department's cybersecurity policies.
- **Serves as liaison** between CISO, OCIT technical staff, and Department to annually review and test Business Continuity, Disaster Recovery, and Cyber Incident Response Plan (CIRP).
- **Serves as liaison** between CISO and Department for communicating cybersecurity and privacy policy to staff and submitting cybersecurity exemption policy requests via the approved process.

All other departments:

- **Serves as liaison** between CISO, County Privacy Officer and Department for issues pertaining to cybersecurity and privacy.
- Responsible for the maintenance of departmental CSP, and ensures cybersecurity policies, processes and procedures shall be at least as comprehensive but may be more stringent than the County's.
- **Serves as liaison** with technical staff for the implementation of technical controls and remediation of technical findings from cybersecurity assessments, audits and cybersecurity incidents.
- Annually reviews and approves the Department's cybersecurity policies.
- Conducts reviews and testing with the County CISO of Business Continuity, Disaster Recovery and Cyber Incident Response Plans (CIRP)
- Responsible for communicating this policy to their users and submitting cybersecurity exemption policy requests via the approved process.
- Maintains confidential and accurate records related to Cyber and Privacy Incidents.

6.8 DEPARTMENT CUSTODIAN OF RECORDS

- Point of contact for department regarding PRA issues

- Facilitates access to departmental records.
- For e-Discovery matters works directly with the Enterprise e-Discovery Manager and refers all Security, HR investigations back to the Enterprise e-Discovery Manager and follows the approved e-Discovery processes.
- Consults with County Counsel about the application of legal requirements for managing the department records, and applicable data retention policies and procedures.
- Maintains records as required by “Legal Hold” and data “Preservation” actions in conjunction with legal matters.
- Compiles the necessary data in response to Public Records Act (PRA) inquiries.
- Collaborates with the County Counsel for legal matters.
- Collaborates with CEO/HR/County Counsel regarding redactions.
- Collaborates with the County Risk Management and County Counsel regarding claims for and against the County.
- Collaborates with the OCIT – Enterprise Security for collection and redaction of applicable County Data when responding to Public Records Act (PRA) inquiries

6.9 CYBERSECURITY JOINT TASK FORCE

- Serves as a joint advisory body to the IT Executive Council on all matters of cybersecurity policy and procedure development, implementation and enforcement.
- Conducts annual review of the County CSP and provide recommendations for changes.

6.10 COUNTY CYBER RESILIENCE MANAGER

- Coordinates with departments to perform annual self-assessments based on Department of Homeland Security (DHS) Cyber Resilience Review.
- Assists departments with scheduling and preparation for third party cybersecurity audits.
- Provides cybersecurity assessment for departments in order to help remediate issues prior to audits and assist with remediation of findings post audit.
- Manages GRC platform to oversee plan of action and milestone tracking for remediation of identified gaps.
- Provides assistance with development of scopes for penetration testing, vulnerability scans and cybersecurity audits.
- Provide department support and coordinates for disaster recovery planning and testing.

6.11 COUNTY PRIVACY OFFICER

- Provides oversight, development, implementation and review of the County privacy programs.
- Provides oversight of the Data Loss Prevention policies and procedures.
- Oversees County Cybersecurity Awareness Training and HIPAA, PII, PHI, and other Privacy and Security trainings.
- Conducts HIPAA compliance reviews and ensures departments are in compliance with all applicable privacy regulations.
- Supports Contracts and Procurement to ensure appropriate privacy and security language is in place to protect and safeguard County data.
- Establishes reporting methods to detect privacy incidents, conduct investigations, breach risk assessments and develop corrective action plans.
- Coordinates notification to state, federal and breach affected individuals and assist departments with regulatory privacy audits.

6.12 COUNTY E-DISCOVERY/PUBLIC RECORDS ACT MANAGER

- Oversees the County's IT Security e-Discovery program and acts as the in-house IT Security e-Discovery consultant for all departments.
- Conducts investigations and manages the production of Root Cause Analysis for cybersecurity incidents.
- Provides oversight and support coordination for e-Discovery services.
- Provides support for handling of digital evidence for Human Resource Services (HRS) investigations.
- Provides e-Discovery litigation support for various legal activities as required by County Counsel or Risk Management departments or their outside Counsels.
- Provides oversight of the vendor forensic services.
- Provides oral and written testimonies.
- Oversees and manages the IT Security processes for collection, processing and reviews of Public Records Acts requests and coordinates all work with:
 - Custodian of Records
 - County Counsel
 - Public Information Officers
 - Suppliers
 - Various IT teams
- "Public Records" may include any data relating to the conduct of the public's business prepared, owned, used, or retained by the County of Orange.

6.13 COUNTY SECURITY OPERATIONS SERVICE DELIVERY MANAGER

- Oversees OC Data Center (DC) Security Operations Center (SOC).
- Provides oversight of the Network Security Software and Appliances Policy.
- Provides support for the cyber incident identification, isolation, eradication, and remediation process.
- Coordinates with departments the delivery for security related initiatives and security operational issues.
- Provides support for security appliances and tools (HDLP, NDLP, IDS/IPS, firewalls, e-mail gateway, and web proxy services).
- Coordinates the County Disaster Recovery testing and implementation.

6.14 COUNTY PUBLIC INFORMATION OFFICE

- The County Public Information Office (PIO) works in coordination with the CISO and County Privacy Officer on any proposed notification materials to the media.

6.15 SERVICE DESK

- The Service Desk is responsible for opening tickets and forwarding to the appropriate party for resolution.

6.16 COUNTY COUNSEL

- County Counsel (CoCo) provides consultation to the Cyber Incident Response Team as needed or applicable.
- CoCo also provides legal analysis or county counsel opinion as needed regarding local, State, Federal, and contractual obligations.

6.17 COUNTY RISK MANAGER

- Point of contact for Cyber Insurance Provider

6.18 COUNTY DATA CENTER MANAGER

- Oversees County of Orange Data Center
- Coordinates with departments the delivery for information technology related initiatives and operational issues.

6.19 HUMAN RESOURCES MANAGER

- Point of contact for OCIT Security for electronic incidents involving County employees.

6.20 VENDORS

- Comply with County and departmental policies, standards and procedures.

6.21 END USERS

- Comply with County and departmental policies, standards and procedures.

7 COUNTY CYBERSECURITY PROGRAM

A strong cybersecurity position is achievable through the implementation, application and management of an effective cybersecurity program. To maintain a strong cybersecurity position, it is essential for cybersecurity programs to include procedures and controls implemented within each department to secure data and information systems.

7.1 CYBERSECURITY PROGRAM DOMAINS

The policies and procedures shall be organized into the following ten domains:

Domain	Description	Reference
Asset Management	Identify, document, and manage assets (people, information, technology, facilities) during their life cycle to ensure sustained productivity to support critical services.	<i>Section 8</i>
Control Management	Identify, analyze, and manage controls in a critical service's operating environment.	<i>Section 9</i>
Configuration & Change Management	Establish processes to ensure the integrity of assets using change control and change control audits.	<i>Section 10</i>
Vulnerability Management	Identify, analyze, and manage vulnerabilities in a critical service's operating environment.	<i>Section 11</i>
Incident Management	Establish processes to identify and analyze events, detect incidents, and determine an organizational response.	<i>Section 12</i>
Service Continuity Management	Ensure the continuity of essential operations of services and their associated assets if a disruption occurs as a result of an incident, disaster, or other disruptive event.	<i>Section 13</i>
Risk Management	Identify, analyze, and mitigate risks to critical service assets that could adversely affect the operation and delivery of services.	<i>Section 14</i>
External Dependencies Management	Establish processes to manage an appropriate level of controls to ensure the sustainment and protection of services and assets that are dependent on the actions of external entities.	<i>Section 15</i>
Training and Awareness	Develop skills and promote awareness for people with roles that support the critical service.	<i>Section 16</i>
Situational Awareness	Actively discover and analyze information related to immediate operational stability and security and to coordinate such information across the enterprise to ensure that all organizational units are performing under a common operating picture.	<i>Section 17</i>

7.2 COUNTY CYBERSECURITY PROGRAM POLICY STATEMENTS

- 7.2.1 Each department shall develop, implement and maintain a departmental cybersecurity program. The procedures and controls included in the departmental cybersecurity program shall be determined by each department and include, at a minimum, the controls identified in this policy. A department may adopt OCIT's cybersecurity program to adhere to this policy.
- 7.2.2 Each department shall designate a Department Information Security Officer (DISO), who is responsible for management of information security issues for that department. Each department decides which appropriate qualifications and criteria are to be used for selection of a DISO. Refer to *Roles & Responsibilities – DISO* for more information on their responsibilities.
- 7.2.3 Each department shall ensure that all County workforce members within its organization comply with the *County Information Technology Usage Policy*.
- 7.2.4 Each department shall review, on an annual basis, departmental cybersecurity program policies and procedures to ensure ongoing compliance with County cybersecurity policies and procedures. Departmental cybersecurity program policies and procedures shall be updated based on this review.
- 7.2.5 All departments shall inform the CISO/DISO when developing or modifying data access methods that involves confidential data including: information processing facilities (regarding physical security controls) and applications (processing and/or storing confidential data) to ensure consistency with existing and anticipated IT cybersecurity policies.
- 7.2.6 Department management is responsible for ensuring that department activities are in compliance with this Policy.
- 7.2.7 The departmental Cybersecurity Program shall be assessed annually alternating between an external assessment, self-assessment, and an assisted or internal assessment. The results of these assessments shall be entered into the County's GRC platform.

8 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.

8.1 GOALS AND OBJECTIVES

- 8.1.1 Services are identified and prioritized.
- 8.1.2 Assets are inventoried, and the authority and responsibility for these assets is established.
- 8.1.3 The relationship between assets and the services they support is established.
- 8.1.4 The asset inventory is managed.
- 8.1.5 Access to assets is managed.
- 8.1.6 Information assets are categorized and managed to ensure the sustainment and protection of the critical service.
- 8.1.7 Facility assets supporting the critical service are prioritized and managed.

8.2 ASSET MANAGEMENT POLICY STATEMENTS

8.2.1 Services Inventory

- 8.2.1.1 Departments shall maintain an inventory of its services. This listing shall be used by the department to assist with its risk management analysis.

8.2.2 Asset Inventory – Information

- 8.2.2.1 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.
- 8.2.2.2 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.
- 8.2.2.3 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.

8.2.3 Asset Inventory - Technology (Devices, Software)

8.2.3.1 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.

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

8.2.3.3 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)

8.2.3.4 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.

8.2.4 Asset Inventory - Facilities

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

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

8.2.5 Access Controls

Refer to *User Provisioning Policy* for additional guidance.

8.2.5.1 Departments shall establish a procedure that ensures only users with legitimate business needs to access County IT resources are provided with user accounts.

8.2.5.2 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.

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

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

- 8.2.5.4 The owner of each County system, or their designee, provides written authorization for all internal and external user access.
- 8.2.5.5 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.
- 8.2.5.6 All County workforce members are to be assigned a unique user ID to access the network.
- 8.2.5.7 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.
- 8.2.5.8 User accounts shall not be shared with others including, but not limited to, someone whose access has been denied or terminated.
- 8.2.5.9 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.

8.2.6 Asset Sanitation/Disposal

- 8.2.6.1 Unless approved by County management, no County computer equipment shall be removed from the premises.
- 8.2.6.2 Prior to re-deployment, storage media shall be appropriately cleansed to prevent unauthorized exposure of data.
- 8.2.6.3 Surplus, donation, disposal or destruction of equipment containing storage media shall be appropriately disposed according to the terms of the equipment disposal services contract.
- 8.2.6.4 Sanitization methods for media containing County information shall be in accordance with NSA standards (for example, clearing, purging, or destroying).
- 8.2.6.5 Disposal of equipment shall be done in accordance with all applicable County, state or federal surplus property and environmental disposal laws, regulations or policies.

Refer to *County of Orange Cybersecurity Best Practices Manual – Technical Controls: Asset Management* for additional guidance.

8.3 RELATED DOCUMENTS

- 8.3.1 County of Orange Cybersecurity Best Practices Manual
- 8.3.2 [County Records Management Policy](#)
- 8.3.3 User Provisioning Policy

9 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.

9.1 GOALS AND OBJECTIVES

- 9.1.1 Control objectives are established.
- 9.1.2 Controls are implemented.
- 9.1.3 Control designs are analyzed to ensure they satisfy control objectives.
- 9.1.4 Internal control system is assessed to ensure control objectives are met.

9.2 CONTROL MANAGEMENT POLICY STATEMENTS

9.2.1 Physical and Environmental Security

- 9.2.1.1 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.
- 9.2.1.2 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.
- 9.2.1.3 Physical protection measures against damage from external and environmental threats shall be implemented by all departments as appropriate.
- 9.2.1.4 Access to any office, computer room, or work area that contains sensitive information shall be physically restricted from unauthorized access.
- 9.2.1.5 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.
- 9.2.1.6 Continuity of power shall be provided to maintain the availability of critical equipment and information systems.
- 9.2.1.7 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.
- 9.2.1.8 Equipment shall be properly maintained to ensure its continued availability and integrity.
- 9.2.1.9 All shared IT infrastructure by more than one department shall meet countywide security policy for facility standards, availability, access, data & network security.

9.2.2 Network Segmentation

NOTE: This section is applicable to Departments that manage their own network devices.

- 9.2.2.1 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.
- 9.2.2.2 Segment the network into multiple, separate zones based on the devices (servers, workstations, mobile devices, printers, etc.) connected to the network.
- 9.2.2.3 Create separate network segments (e.g., VLANs) for BYOD (bring your own device) systems or other untrusted devices.
- 9.2.2.4 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.

9.2.3 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:

- 9.2.3.1 Establish and manage a process for authorizing, issuing and tracking the use of MCDs.
- 9.2.3.2 Permit only authorized MCDs to connect to County information assets or networks that store, process, transmit, or connects to County information and information assets.
- 9.2.3.3 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.
- 9.2.3.4 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.
- 9.2.3.5 Ensure that MCDs are configured to restrict the user from circumventing the authentication process.
- 9.2.3.6 Provide security awareness training to County employees that informs MCD users regarding MCD restrictions.
- 9.2.3.7 Label MCDs with County address and/or phone number so that the device can be returned to the County if recovered.
- 9.2.3.8 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.

9.2.4 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.

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

approved.

- 9.2.4.2 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.
- 9.2.4.3 The County will respect the privacy of a user's voluntary use of a personally owned device to access County IT resources.
- 9.2.4.4 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.

9.2.5 Logon Banners and Warning Notices

- 9.2.5.1 At the time of network login, the user shall be presented with a login banner.
- 9.2.5.2 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.
- 9.2.5.3 Warning banners shall remain on the screen until the user takes explicit actions to log on to the information system.
- 9.2.5.4 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.
- 9.2.5.5 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.

9.2.6 Authentication

- 9.2.6.1 Authenticate user identities at initial connection to County resources.
- 9.2.6.2 Authentication mechanisms shall be appropriate to the sensitivity of the information contained.
- 9.2.6.3 Users shall not receive detailed feedback from the authenticating system on failed logon attempts.

9.2.7 Passwords

- 9.2.7.1 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).
- 9.2.7.2 Passwords are a primary means to control access to systems and shall therefore be selected, used, and managed to protect against unauthorized discovery or usage. Passwords shall satisfy the following complexity rule:

- Passwords will contain a minimum of one upper case letter
- Passwords will contain a minimum of one lower case letter
- Passwords will contain a minimum of one number: 1- 0
- Passwords will contain a minimum of one symbol: !, @, #, \$, %, ^, &, *, (,)
- Password characters will not be sequential (Do not use: ABCD , This is ok: ACDB)
- Password characters will not be repeated in a row (Do not use: P@\$\$\$. This is ok: P@\$\$)
- COMPLEX PASSWORD EXAMPLE: P@\$SWoRd13

- 9.2.7.3 Passwords shall have a minimum length of 8 characters.
- 9.2.7.4 Passwords shall not be reused for twelve iterations.
- 9.2.7.5 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.
- 9.2.7.6 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.
- 9.2.7.7 Newly-created accounts shall be assigned a randomly generated password prior to account information being provided to the user.
- 9.2.7.8 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.
- 9.2.7.9 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.
- 9.2.7.10 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.
- 9.2.7.11 All passwords are to be treated as sensitive information.
- 9.2.7.12 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.
- 9.2.7.13 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.

9.2.8 Inactivity Timeout and Restricted Connection Times

- 9.2.8.1 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.
- 9.2.8.2 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.

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

9.2.9 Account Monitoring

- 9.2.9.1 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.)
- 9.2.9.2 The control mechanisms for all types of access to County IT resources by contractors, customers or vendors are to be documented.
- 9.2.9.3 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.
- 9.2.9.4 After a longer period, such as 60 days, the account shall be disabled by the system when the technology is feasible or available.
- 9.2.9.5 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.

9.2.10 Administrative Privileges

Refer to *Use of Administrative Accounts by System Administrators and End Users Policy* for additional guidance.

- 9.2.10.1 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.
- 9.2.10.2 Administrative accounts shall only be granted to individuals who have a job requirement to conduct systems administration tasks.
- 9.2.10.3 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.
- 9.2.10.4 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.
- 9.2.10.5 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.
- 9.2.10.6 All passwords for privileged system-level accounts (e.g., root, enable, OS admin, application administration accounts, etc.) shall comply with Section 9.2.8.

9.2.11 Remote Access

- 9.2.11.1 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.
- 9.2.11.2 Remote access privileges shall be granted to County workforce members only for legitimate business needs and with the specific approval of department management.

- 9.2.11.3 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.
- 9.2.11.4 Remote sessions shall be terminated after 15 minutes of inactivity requiring the user to authenticate again to access County resources.
- 9.2.11.5 All remote access infrastructures shall include the capability to monitor and record a detailed audit trail of each remote access attempt.
- 9.2.11.6 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.
- 9.2.11.7 Periodic assessments shall be performed to identify unauthorized remote connections. Results shall be used to address any vulnerabilities and prioritized according to criticality.
- 9.2.11.8 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.
- 9.2.11.9 Users attempting to use external remote access shall utilize a County-approved multi-factor authentication process.
- 9.2.11.10 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).
- 9.2.11.11 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.

9.2.12 Wireless Access

- 9.2.12.1 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.
- 9.2.12.2 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.
- 9.2.12.3 County data that is transmitted over any wireless network shall be protected in accordance with the sensitivity of the information.
- 9.2.12.4 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.
- 9.2.12.5 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.

9.2.13 System and Network Operations Management

- 9.2.13.1 Operating procedures and responsibilities for all County information processing facilities shall be formally authorized, documented, and updated.
- 9.2.13.2 Departments shall establish controls to ensure the security of the information systems networks that they operate.
- 9.2.13.3 Operational system documentation for County information systems shall be protected from unauthorized access.
- 9.2.13.4 System utilities shall be available to only those users who have a business case for accessing the specific utility.

9.2.14 System Monitoring and Logging

- 9.2.14.1 Systems operational staff shall maintain appropriate log(s) of activities, exceptions and information security events involving County information systems and services.
- 9.2.14.2 Each department shall maintain a log of all faults involving County information systems and services.
- 9.2.14.3 Logs shall be protected from unauthorized access or modifications wherever they reside.
- 9.2.14.4 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.
- 9.2.14.5 Auditing and logging of user activity shall be implemented on all critical County systems that support user access capabilities.
- 9.2.14.6 Periodic log reviews of user access and privileges shall be performed in order to monitor access of sensitive information.

9.2.15 Malware Defenses

- 9.2.15.1 Departments shall implement endpoint security on computing devices connected to the County network. Endpoint security may include one or more of the following software: anti-virus, anti-spyware, personal firewall, host-based intrusion detection (IDS), network-based intrusion detection (IDS), intrusion prevention systems (IPS), and white listing and black listing of applications, web sites, and IP addresses.
- 9.2.15.2 Special features designed to filter out malicious software contained in either email messages or email attachments shall be implemented on all County email systems.
- 9.2.15.3 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.

9.2.16 Data Loss Prevention

- 9.2.16.1 Departments shall implement host-based Data Loss Prevention (DLP) to reduce the risk of data breach related to sensitive information.
- 9.2.16.2 Departments shall deploy encryption software on mobile devices containing sensitive. See Section 9.2.19 Encryption for additional guidance.

9.2.17 Data Transfer

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

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

9.2.18 Encryption

9.2.18.1 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.

9.2.18.2 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.

9.2.18.3 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.

9.2.18.4 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

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

9.2.19 System Acquisition and Development

9.2.19.1 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).

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

9.2.19.3 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.

9.2.19.4 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.

9.2.19.5 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

9.2.19.6 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

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

9.2.19.8 Clear-text data that results from testing shall be handled, stored, and disposed of in the same

manner and using the same procedures as are used for production data.

- 9.2.19.9 System tests shall be performed on data that is constructed specifically for that purpose.
- 9.2.19.10 System testing shall not be performed on operational data unless the necessary safeguards are in place.
- 9.2.19.11 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

- 9.2.19.12 The development of software for use on County information systems shall have documented change control procedures in place to ensure proper versioning and implementation.
- 9.2.19.13 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.
- 9.2.19.14 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.
- 9.2.19.15 Systems shall be hardened, and logs monitored to ensure the avoidance of the introduction and exploitation of malicious code.
- 9.2.19.16 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.
- 9.2.19.17 In conjunction with other access control policies, any opportunity for information leakage shall be prevented through good system design practices.
- 9.2.19.18 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:

- 9.2.19.19 Baseline configuration shall incorporate Principle of Least Privilege and Functionality.
- 9.2.19.20 Systems shall be deployed where feasible to utilize existing County authentication methods.
- 9.2.19.21 Session inactivity timeouts shall be implemented for all access into and from County networks.
- 9.2.19.22 All applications are to have access controls unless specifically designated as a public access resource.
- 9.2.19.23 Meet the password requirements defined in Section 9.2.8: Passwords.
- 9.2.19.24 Strictly control access enabling only privileged users or supervisors to override system controls or the capability of bypassing data validation or editing problems.
- 9.2.19.25 Monitor special privilege access, e.g. administration accounts.
- 9.2.19.26 Restrict authority to change master files to persons independent of the data processing function.

- 9.2.19.27 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.
- 9.2.19.28 Be capable of routinely monitoring the access to automated systems containing County Information.
- 9.2.19.29 Log all modifications to the system files.
- 9.2.19.30 Limit access to system utility programs to necessary individuals with specific designation.
- 9.2.19.31 Maintain audit logs on a device separate from the system being monitored.
- 9.2.19.32 Delete or disable all default accounts.
- 9.2.19.33 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.
- 9.2.19.34 Restrict access to server-file-system controls that allow access to other users' files.
- 9.2.19.35 Ensure that servers containing user credentials shall be physically protected, hardened and monitored to prevent inappropriate use.

9.2.20 Procurement Controls

- 9.2.20.1 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.

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

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

9.2.21 IT Services Provided to Public

- 9.2.21.1 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.

9.2.22 Removable Media

- 9.2.22.1 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 requirements.

Refer to County of Orange Cybersecurity Best Practices Manual – Technical Controls: Control Management for additional guidance.

9.3 RELATED DOCUMENTS

- 9.3.1 County of Orange Cybersecurity Best Practices Manual – Technical Controls: Control Management
- 9.3.2 [CRR Supplemental Resource Guide – Controls Management](#)
- 9.3.3 [CERT Resilience Management Model](#)
- 9.3.4 Use of Administrative Accounts by System Administrators and End Users Policy

10 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.

10.1 GOALS AND OBJECTIVES

- 10.1.1 The lifecycle of assets is managed.
- 10.1.2 The integrity of technology and information assets is managed.
- 10.1.3 Asset configuration baselines are established.

10.2 CONFIGURATION & CHANGE MANAGEMENT POLICY STATEMENTS

- 10.2.1.1 Changes to all information processing facilities, systems, software, or procedures shall be strictly controlled according to formal change management procedures.
- 10.2.1.2 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*.
- 10.2.1.3 Only authorized users shall make any changes to system and/or software configuration files.
- 10.2.1.4 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.
- 10.2.1.5 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.

- 10.2.1.6 Each department shall conduct periodic audits designed to determine if unauthorized software has been installed on any of its computers.
- 10.2.1.7 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.
- 10.2.1.8 Production computing environments shall be separated from development and test computing environments to reduce the risk of one environment adversely affecting another.
- 10.2.1.9 System capacity requirements shall be monitored, and usage projected to ensure the continual availability of adequate processing power, bandwidth, and storage.
- 10.2.1.10 System acceptance criteria for all new information systems and system upgrades shall be defined, documented, and utilized to minimize risk of system failure.

Refer to *County of Orange Cybersecurity Best Practices Manual – Technical Controls: Configuration and Change Management* for additional guidance.

10.3 RELATED DOCUMENTS

- 10.3.1 County of Orange Cybersecurity Manual – Technical Controls: Configuration and Change Management
- 10.3.2 County Security Review and Approval Process
- 10.3.3 [CRR Supplemental Resource Guide – Configuration & Change Management](#)
- 10.3.4 [CERT Resilience Management Model](#)

11 VULNERABILITY MANAGEMENT

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

11.1 GOALS AND OBJECTIVES

- 11.1.1 Preparation for vulnerability analysis and resolution activities is conducted.
- 11.1.2 A process for identifying and analyzing vulnerabilities is established and maintained.
- 11.1.3 Exposure to identified vulnerabilities is managed.
- 11.1.4 The root causes of vulnerabilities are addressed.

11.2 VULNERABILITY MANAGEMENT POLICY STATEMENTS

- 11.2.1.1 Departments shall develop and maintain a vulnerability management process as part of its Cybersecurity Program.

Refer to *County of Orange Cybersecurity Best Practices Manual – Technical Controls: Vulnerability Management* for additional guidance.

11.3 RELATED DOCUMENTS

- 11.3.1 County of Orange Cybersecurity Best Practices Manual – Technical Controls: Vulnerability Management
- 11.3.2 County Vulnerability Management Policy
- 11.3.3 County Patch Management Policy
- 11.3.4 [CRR Supplemental Resource Guide – Vulnerability Management](#)
- 11.3.5 [CERT Resilience Management Model](#)

12 CYBERSECURITY INCIDENT MANAGEMENT

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

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

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

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

12.1 GOALS AND OBJECTIVES

- 12.1.1 A process for identifying, analyzing, responding to, and learning from incidents is established.
- 12.1.2 A process for detecting, reporting, triaging, and analyzing events is established.
- 12.1.3 Incidents are declared and analyzed.
- 12.1.4 A process for responding to and recovering from incidents is established.
- 12.1.5 Post-incident lessons learned are translated into improvement strategies.

12.2 CYBERSECURITY INCIDENT MANAGEMENT POLICY STATEMENTS

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

- System preparation
- Problem identification
- Problem containment
- Problem eradication
- Incident recovery
- Lessons learned

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

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

- 12.2.1.4 Departments shall conduct periodic (at least annually) cybersecurity incident scenario sessions for personnel associated with the cybersecurity incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the cybersecurity incident handling team.
- 12.2.1.5 Departments shall develop and document procedures for reporting cybersecurity incidents. For example, all employees, contractors, vendors and customers of County information systems shall be required to note and report any observed or suspected security weaknesses in systems to management. In the event a department has not established these procedures, the department may adopt the *County's Cyber Incident Response Plan*.
- 12.2.1.6 Each department shall familiarize its employees on the use of its cybersecurity incident reporting procedures.
- 12.2.1.7 Contact with local authorities, including law enforcement, shall be conducted through an organized, repeatable process that is both well documented and communicated.
- 12.2.1.8 Contact with special interest groups, including media and labor relations, shall be conducted through an organized, repeatable process that is both well documented and communicated.
- 12.2.1.9 Where a follow-up action against an entity after a cybersecurity incident shall involve civil or criminal legal action, evidence shall be collected, retained, and presented to conform to the rules for evidence as demanded by the relevant jurisdiction(s). At the Department's discretion, they may obtain the services of qualified external professionals to complete these tasks.
- 12.2.1.10 Departments shall report cybersecurity incidents to the Central IT Service Desk in accordance with the *County's Cyber Incident Reporting Policy*.
- 12.2.1.11 Confirmed cybersecurity incidents that meet the criteria defined in the *Significant Incident/Claim Reporting Protocol* shall be reported by the County's Chief Information Security Officer to the Chief Information Officer (CIO), County Executive Officer (CEO), and the Board of Supervisors within 24 hours of determination that a cybersecurity incident has occurred.

Refer to *County of Orange Cybersecurity Best Practices Manual – Technical Controls: Cyber Incident Management* for additional guidance.

12.3 RELATED DOCUMENTS & REFERENCES

- 12.3.1 County of Orange Cybersecurity Best Practices Manual – Technical Controls: Cyber Incident Management
- 12.3.2 County Cyber Incident Response Plan
- 12.3.3 County Cyber Incident Reporting Policy
- 12.3.4 [CRR Supplemental Resource Guide – Incident Management](#)
- 12.3.5 [CERT Resilience Management Model](#)

13 SERVICE CONTINUITY MANAGEMENT

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

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

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

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

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

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

13.1 GOALS AND OBJECTIVES

- 13.1.1 Service continuity plans for high-value services are developed.
- 13.1.2 Service continuity plans are reviewed to resolve conflicts between plans.
- 13.1.3 Service continuity plans are tested to ensure they meet their stated objectives.
- 13.1.4 Service continuity plans are executed and reviewed.

13.2 SERVICE CONTINUITY MANAGEMENT POLICY STATEMENTS

- 13.2.1.1 Backups of all essential electronically-maintained County business data shall be routinely created and properly stored to ensure prompt restoration.
- 13.2.1.2 Each department shall implement and document a backup approach for ensuring the availability of critical application databases, system configuration files, and/or any other electronic information critical to maintaining normal business operations within the department.

- 13.2.1.3 The frequency and extent of backups shall be in accordance with the importance of the information and the acceptable risk as determined by each department.
- 13.2.1.4 Departments shall ensure that locations where backup media are stored are safe, secure, and protected from environmental hazards. Access to backup media shall be commensurate with the highest level of information stored and physical access controls shall meet or exceed the physical access controls of the data's source systems.
- 13.2.1.5 Backup media shall be labeled and handled in accordance with the highest sensitivity level of the information stored on the media.
- 13.2.1.6 Departments shall define and periodically test a formal procedure designed to verify the success of the backup process.
- 13.2.1.7 Restoration from backups shall be tested initially once the process is in place and periodically afterwards. Confirmation of business functionality after restoration shall also be tested in conjunction with the backup procedure test.
- 13.2.1.8 Departments shall retain backup information only as long as needed to carry out the purpose for which the data was collected, or for the minimum period required by law.
- 13.2.1.9 Alternate storage facilities shall be used to ensure confidentiality, integrity and availability of all County systems.
- 13.2.1.10 Each department shall develop, periodically update, and regularly test business continuity and disaster recovery plans in accordance with the County's Business Continuity Management Policy.
- 13.2.1.11 Departments shall review and update their Risk Assessments (RAs) and Business Impact Analyses (BIAs) as necessary, determined by department management (annually is recommended). As detailed in Section 14: Risk Assessment and Treatment, RAs include department identification of risks that can cause interruptions to business processes along with the probability and impact of such interruptions and the consequences to information security. A BIA establishes the list of processes and systems that the department has deemed critical after performing a risk analysis.
- 13.2.1.12 Continuity plans shall be developed and implemented to provide for continuity of business operations in the event that critical IT assets become unavailable. Plans shall provide for the availability of information at the required level and within the established Recovery Time Objective (RTO) and their location, as alternate facilities shall be used to maintain continuity.
- 13.2.1.13 Each department shall maintain a comprehensive plan document containing its business continuity plans. Plans shall be consistent, address information security requirements, and identify priorities for testing and maintenance. Plans shall be prepared in accordance with the standards established by the County's Business Continuity Management Policy.
- 13.2.1.14 Each department shall define failure prevention protocols to maintain confidentiality, integrity and availability. Departments shall automate failover procedures where applicable and maintain adequate (predictable) levels of ancillary components to meet this provision.

Refer to *County of Orange Cybersecurity Best Practices Manual – Technical Controls: Service Continuity Management* for additional guidance.

13.3 RELATED DOCUMENTS

- 13.3.1 County of Orange Cybersecurity Best Practices Manual – Technical Controls: Service Continuity Management

13.3.2 County Business Continuity Plan

13.3.3 [CRR Supplemental Resource Guide – Service Continuity Management](#)

13.3.4 [CERT Resilience Management Model](#)

13.3.5 [Insert data retention policy](#)

14 RISK MANAGEMENT

Risk assessments shall identify, quantify, and prioritize risks against County assets, systems, processes and deliverables. The results shall guide and determine the priorities for information security risk management and for implementing controls selected to protect against risks. Mitigation of risks furthers the County's goal of protecting its assets from harm.

Risk management is a foundational activity for any organization and is practiced at all levels of the organization, from the executives down to individuals within business units. Organizations shall manage many different types of risk to remain effective and achieve their objectives. The pervasiveness of the threats to information and the dynamics of today's global operational environment require ongoing collaboration facilitated by two-way internal and external communication.

To effectively manage operational risk, organizations shall establish processes to:

- identify risks to which the organization is exposed
- analyze risks and determine appropriate risk disposition
- control risks to reduce probability of occurrence and/or minimize impact
- monitor risks and responses to risks and improve the organization's capabilities for managing current and future risks

The risk management process involves:

- Create a Risk Management Plan—Outlines a strategy and plan creation process and identifies issues and considerations to help ensure that the plan addresses the organization's risk management needs
- Implement the Risk Plan—Outlines the process for ensuring that the organization's risk management plan is implemented and meets the standards set by the organization
- Monitor and Improve Operational Risk Management—Outlines the process and considerations for keeping the risk management process resilient and robust
- Risk-Based Approach

14.1 GOALS AND OBJECTIVES

14.1.1 A strategy for identifying, analyzing, and mitigating risks is developed.

14.1.2 Risk tolerances are identified, and the focus of risk management activities is established.

14.1.3 Risks are identified.

14.1.4 Risks are analyzed and assigned a disposition.

14.1.5 Risks to assets and services are mitigated and controlled.

14.2 RISK MANAGEMENT POLICY STATEMENTS

Department responsibility not IT

14.2.1.1 Departments shall develop and implement risk assessment policies and procedures based on the *County's Risk Management Process* that shall include the systematic approach of estimating the magnitude of risks (risk analysis) and the process of comparing the estimated risks against risk criteria to determine the significance of the risks (risk evaluation).

14.2.1.2 Departments shall perform the process of assessing risks and selecting the controls for coverage of multiple organizational information assets or individual information systems.

- 14.2.1.3 Risk assessments shall be performed periodically to address changes in the security requirements and in the risk situation, e.g., changes in assets, threats, vulnerabilities, impacts, or risk evaluation methodologies and when significant infrastructure changes occur. These risk assessments shall be undertaken in a methodical manner capable of producing reproducible results.
- 14.2.1.4 Before considering risk mitigation, the department shall decide criteria for determining whether or not risks can be accepted. Risks may be accepted if, for example, it is assessed that the risk is low or that the cost of mitigation is not cost-effective for the department.
- 14.2.1.5 For each of the risks identified following the risk assessment, a risk mitigation decision needs to be made. Possible options for risk mitigation include:
- Accept – an explicit or implicit decision not to take action that would affect a particular risk
 - Avoid – a strategy or measure that effectively removes the exposure of an organization to a risk
 - Control/Mitigate – deliberate actions taken to reduce a risk’s potential for harm or to maintain the risk at an acceptable level
 - Defer/Monitor – an explicit decision to further research and defer action on a risk until the need to address it is apparent and the risk is better understood
 - Transfer – shifting some or all of the risk to another entity, asset, system, network, or geographic area
- 14.2.1.6 For those risks where the risk mitigation decision has been to apply appropriate controls, these controls shall be selected and implemented to meet the requirements identified by the risk assessment. Controls shall ensure that risks are reduced to an acceptable level, taking into account:
- Requirements and constraints of County, state and federal legislation and regulations
 - Organizational objectives
 - Operational requirements and constraints
 - Cost of implementation and operation in relation to the risks being reduced and keeping mitigation costs proportional to the organization’s requirements and constraints
 - Need to balance the investment in implementation and operation of controls against the harm likely to result from security failures

Refer to County of Orange Cybersecurity Best Practices Manual – Processes: County Risk Management Process for additional guidance.

14.3 RELATED DOCUMENTS

- 14.3.1 County of Orange Cybersecurity Best Practices Manual – Processes: County Risk Management Process
- 14.3.2 County Risk Management Process
- 14.3.3 [CRR Supplemental Resource Guide – Risk Management](#)
- 14.3.4 [CERT Resilience Management Model](#)

15 EXTERNAL DEPENDENCIES MANAGEMENT

In today's technology and business environment, organizations often rely on outside entities, including technology vendors, suppliers of raw materials, shared public infrastructure, and other public services that support the organization. External dependencies management (EDM) focuses on establishing an appropriate level of controls to manage the risks that originate from or are related to the organization's dependence on these external entities. The purpose of EDM is to ensure the protection and sustainment of services and assets that are dependent on the actions of external entities.

Identifying, prioritizing, and managing relationships with external entities over their entire lifecycle are foundational activities for the development of effective risk mitigation and disposition strategies. To effectively manage external dependencies, organizations shall establish:

- a strategy and basic plan for EDM
- key processes for identifying, prioritizing, monitoring, and tracking external dependencies
- guidance and procedures on the formation of relationships with external entities
- an approach for managing and governing existing external entity relationships
- ongoing oversight, reporting, and correction of external entity performance
- an approach for improving the organization's EDM processes and program

Like many key resilience practices, EDM shall be thought of as a planned, continuous process. In the case of EDM in particular, many organizations may have only ad hoc or incomplete processes around forming new relationships with external entities or around managing existing relationships. It is also not unusual for particular organizations to have detailed procedures around the formation of new relationships, but for the ongoing management of relationships to run according to a substantially different set of objectives or standards. Effective EDM requires standard, planned guidance across the entire lifecycle of external entity relationships and continuous monitoring and improvement of the approach.

15.1 GOALS AND OBJECTIVES

- 15.1.1 External dependencies are identified and prioritized to ensure sustained operation of high-value services.
- 15.1.2 Risks due to external dependencies are identified and managed.
- 15.1.3 Relationships with external entities are formally established and maintained.
- 15.1.4 Performance of external entities is managed.
- 15.1.5 Dependencies on public services and infrastructure service providers are identified.

15.2 EXTERNAL DEPENDENCIES MANAGEMENT POLICY STATEMENTS

THIS SECTION RELATED TO IT ONLY

- 15.2.1.1 Departments contracting with business partners, such as contractors, consultants or vendors, shall use the guidelines from this policy to ensure the safeguarding of County information systems. These contracts shall be reviewed for appropriate compliance with County cybersecurity policies.
- 15.2.1.2 Departments shall review applicable equipment and service purchases to ensure that vendors and contractors are aware of and are in compliance with County cybersecurity policy. Departments shall obtain documentation supporting the business partners, contractors,

consultants, or vendors compliance with County's cybersecurity policies including:

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

- 15.2.1.3 External users (contractors, vendors and customers) who are not already covered by an existing agreement shall sign non-disclosure agreements prior to being given access to sensitive information.
- 15.2.1.4 Risk assessment and identification shall take place prior to establishing vendor, customer or contractor access to County information systems and shall be in accordance with the policy set forth in this document.
- 15.2.1.5 Contractors and vendors who have access to Personal Identifiable Information, as defined herein, shall comply with the California Information Practices Act and the Consumer Credit Reporting Act, as applicable.
- 15.2.1.6 Agreements or contracts with a vendor, contractor or customer that involves access to sensitive information resources shall contain sections that delineate County information security issues relevant to that business access and require the vendor, contractor and/or customer to adhere to County IT Security Policy. If Security is outsourced, the vendor shall demonstrate a standard of care as this shall also be reflected in the vendor contract.
- 15.2.1.7 Confidentiality and non-disclosure agreements shall be reviewed regularly, especially when contracts expire.

15.3 RELATED DOCUMENTS

- 15.3.1 [CRR Supplemental Resource Guide – External Dependencies Management](#)
- 15.3.2 [CERT Resilience Management Model](#)

16 TRAINING & AWARENESS

Training and awareness focuses on the processes by which an organization plans, identifies needs for, conducts, and improves training and awareness to ensure the organization's operational cyber resilience requirements and goals are known and used.

16.1 GOALS AND OBJECTIVES

- 16.1.1 Cybersecurity awareness and training programs are established.
- 16.1.2 Awareness and training activities are conducted.

16.2 TRAINING & AWARENESS POLICY STATEMENTS

- 16.2.1.1 Departments shall assist Human Resources and OCIT Enterprise Privacy and Cybersecurity with ensuring that all County workforce members within its organization (including employees, contractors, consultants, interns, temporary help, and extra help) complete the County's Cybersecurity Awareness Training. The Cybersecurity Awareness Training is to be completed on an annual basis.
- 16.2.1.2 Security awareness training shall address user actions to be utilized to protect information systems and services against malicious software and against the unauthorized execution of mobile code (e.g., ActiveX controls, Java applets).
- 16.2.1.3 Departments shall provide their users with training on the appropriate use of both the Internet and County email systems and on the handling of email messages and attachments. Training shall include acceptance of County's IT Usage Policy by department workforce members including employees, contractors, consultants, interns, and volunteers.

Refer to *County of Orange Cybersecurity Best Practices Manual – Technical Controls: Security Training and Awareness* for additional guidance.

16.3 RELATED DOCUMENTS

- 16.3.1 County of Orange Cybersecurity Best Practices Manual – Technical Controls: Security Training and Awareness
- 16.3.2 [CRR Supplemental Resource Guide – Training & Awareness](#)
- 16.3.3 [CERT Resilience Management Model](#)

17 SITUATIONAL AWARENESS

Situational awareness provides an organization an understanding of its critical service's operating environment and the environment's impact on the operation of the critical service. This understanding provides stakeholders with a sufficiently accurate and up-to-date understanding of the past, current, and projected future state of a critical service and supports effective decision making in the context of a common operating environment. This includes understanding the assets and other services that affect or depend on the critical service. The representation or picture of the state of a critical service (including the condition of its supporting assets, the performance of its high-value physical and cyber processes, and events detected and responded to by its physical and cybersecurity safeguards) is presented to stakeholders in the context of the threat environment (internal and external) and the resulting risks to the critical service's mission.

The situational awareness process establishes a *common operating picture* (COP) by collecting, fusing, and analyzing data to support automated or human decisions about appropriate actions to prevent disruption of a critical service or to restore the service to proper function. This COP is shared through timely communication and presentation of the results of the data analysis to appropriate decision makers (people or machines) in a form that aids human comprehension (e.g., using data visualization techniques, appropriate use of alarms) and allows operators or other personnel to quickly grasp the key elements needed for good decision making.

The COP shall be accurate and actionable (appropriate for supporting good decisions and actions). However, different members of an organization likely need different, and not necessarily complete, views of the operational environment. Depending on how it is presented, a complete picture could present too much information and overload a human decision maker. Operators shall not be presented with a massive data dump; rather, operators shall see only what's important, which is determined by the risk strategy and overall risk picture.

Communication between situational awareness and other organizational processes is bi-directional. Other processes report information, such as vulnerabilities, incidents, and risk management decisions, to the situational awareness process. At the same time, the situational awareness process contributes the information, or improves its quantity or quality, needed by other processes that inform decision making or appropriate actions.

Communication among processes relies on their linkages. These linkages can be simple, such as reporting of suspicious events to the incident response team. They can also be complex, such as asset and controls management processes that include an intrusion detection system (IDS) that monitors assets and services deemed important by the risk management process and alerts those who can take mitigating steps.

The high-level outline below highlights the four phases of this process:

- Plan for Situational Awareness—Highlights the elements necessary for an effective situational awareness plan
- Collect and Analyze Situational Awareness Data—Presents an approach for identifying and managing the requirements for situational awareness data collection and analysis, including recommended categories of information to be monitored to assure organizational resilience and an approach for analyzing situational awareness information
- Communicate Information Needed to Make Appropriate Decisions—Outlines a process that defines steps necessary to manage the communication of information to appropriate staff, enabling them to make informed decisions and identify follow-up actions
- Improve Situational Awareness Processes and Technology—Provides an approach for reviewing and improving the organization's situational awareness capability

Threat intelligence is often presented in the form of Indicators of Compromise (IoCs) or threat feeds. Threat intelligence requires organizations to understand themselves first and then understand the adversary. The County may use information from a variety of intelligence sources to identify and mitigate risks in the current cyberspace. Departments are free to either procure their own Cyber Intelligence services and advisories or they may subscribe to the OCIT provided intelligence services. Intelligence services, at a minimum, shall perform the following:

Impact of Cyber Threats Assessment

The impact of cyber threats is evaluated against the likelihood and possible harm of a potential threat. Analysis includes:

- Probability of each threat occurring.
- Cost if each threat were to actually occur. Costs shall be interpreted broadly to include money, resources, time, and loss of reputation among others.
- Cost, in money or effort, to prepare preemptive mitigation of probable cyber threats.

17.1 GOALS AND OBJECTIVES

17.1.1 Threat monitoring is performed.

17.1.2 The requirements for communicating threat information are established.

17.1.3 Threat information is communicated.

17.2 SITUATIONAL AWARENESS POLICY STATEMENTS

17.2.1.1 The County shall ensure that all systems and systems owners are receiving security alerts, advisories from external parties including: US-CERT, enforcement authorities, vendors.

17.2.1.2 Alerts and advisories shall be disseminated internally and include applicable directives outlining implementation timeframes.

17.2.1.3 Alerts and advisories shall be automated where possible.

17.2.1.4 Departments shall respond to security advisory information received from either internal (e.g., County) or approved external sources by promptly undertaking appropriate and/or recommended procedures intended to mitigate the effects of actual or potential security incidents.

17.3 RELATED DOCUMENTS

17.3.1 [CRR Supplemental Resource Guide – Situational Awareness](#)

17.3.2 [CERT Resilience Management Model](#)

18 DEFINITIONS

Refer to the *Cybersecurity Best Practices Manual – Glossary* for a listing of definitions for terms used in this document.

19 REFERENCES

Document	Issued By
County Patch Management Policy	County of Orange
County Security Review and Approval Process	County of Orange
County Vulnerability Management Policy	County of Orange
Use of Administrative Accounts Policy	County of Orange
Cyber Incident Response Plan	County of Orange
Cyber Incident Reporting Policy	County of Orange
County Risk Management Process	County of Orange
User Provisioning Policy	County of Orange
County Variance Review and Approval Process	County of Orange
CRR Supplemental Resource Guide – Asset Management	Department of Homeland Security
CRR Supplemental Resource Guide – Controls Management	Department of Homeland Security
CRR Supplemental Resource Guide – Configuration & Change Management	Department of Homeland Security
CRR Supplemental Resource Guide – Vulnerability Management	Department of Homeland Security
CRR Supplemental Resource Guide – Incident Management	Department of Homeland Security
CRR Supplemental Resource Guide – Service Continuity Management	Department of Homeland Security
CRR Supplemental Resource Guide – Risk Management	Department of Homeland Security
CRR Supplemental Resource Guide – External Dependencies Management	Department of Homeland Security
CRR Supplemental Resource Guide – Training & Awareness	Department of Homeland Security
CRR Supplemental Resource Guide – Situational Awareness	Department of Homeland Security
Department of Homeland Security Cyber Resilience Review	Department of Homeland Security

APPENDIX A: DEPARTMENT LISTING

Department	Department Code
Assessor	AS
Auditor-Controller	AC
Board of Supervisors District 1	BOS1
Board of Supervisors District 2	BOS2
Board of Supervisors District 3	BOS3
Board of Supervisors District 4	BOS4
Board of Supervisors District 5	BOS5
County Executive Office	CEO
Child Support Services	CSS
Clerk of the Board of Supervisors	COB
Clerk Recorder	CR
County Counsel	COCO
District Attorney	DA
Health Care Agency	HCA
Internal Audit Department	IAD
John Wayne Airport	JWA
OC Community Resources	OCCR
OC Information Technology	OCIT
OC Public Works	OCPW
OC Waste & Recycling	OCWR
Probation	PROB
Public Defender	PD
Registrar of Voters	ROV
Sheriff-Coroner	SC
Social Services Agency	SSA
Treasurer-Tax Collector	TTC

APPENDIX B: FACILITY LISTING



Facility_Listing.xlsx

APPENDIX C: DEVICE TYPE LISTING

Device Type	Device Type Code
Desktop Computers	W
Laptop Computers	L
Tablets (iPads and Android devices)	T
Mobile/Smart Phones (basic cell phones, iPhones, Blackberry, Windows Phones and Android Phones)	M
Servers	S
External Storage Devices	E
Network Switches	N
Routers	R
Firewalls	F
Security Appliances	SA
Internet of Things (IoT) devices	I
Printers	P
Scanners	C
Kiosks and Thin clients	K
Mainframe Hardware	M
Telephones (VoIP)	V

APPENDIX D: POLICY STATEMENT CROSS REFERENCES

CONTROL FAMILY	NUMBER	NIST SP 800-53 CONTROLS	POLICY SECTION(S)
Access Control	AC-1	Access Control Policy and Procedures	
	AC-2	Account Management	
	AC-3	Access Enforcement	
	AC-4	Information Flow Enforcement	
	AC-5	Separation of Duties	
	AC-6	Least Privilege	
	AC-7	Unsuccessful Login Attempts	
	AC-8	System Use Notification	
	AC-9	Previous Logon (Access) Notification	
	AC-10	Concurrent Session Control	
	AC-11	Session Lock	
	AC-14	Permitted Actions without Identification or Authentication	
	AC-17	Remote Access	
	AC-18	Wireless Access	
	AC-19	Access Control for Mobile Devices	
	AC-20	Use of External Information Systems	
	AC-21	User-Based Collaboration and Information Sharing	
	AC-22	Publicly Accessible Content	
	Audit and Accountability	AU-1	Audit and Accountability Policy and Procedures
AU-2		Auditable Events	
AU-3		Content of Audit Records	
AU-6		Audit Review, Analysis, and Reporting	
AU-8		Time Stamps	

CONTROL FAMILY	NUMBER	NIST SP 800-53 CONTROLS	POLICY SECTION(S)
	AU-9	Protection of Audit Information	
	AU-12	Audit Generation	
Awareness and Training	AT-1	Security Awareness and Training Policy and Procedures	
	AT-2	Security Awareness	
	AT-3	Security Training	
Configuration Management	CM-1	Configuration Management Policy and Procedures	
	CM-2	Baseline Configuration	
	CM-3	Configuration Change Control	
	CM-4	Security Impact Analysis	
	CM-5	Access Restrictions for Change	
	CM-6	Configuration Settings	
	CM-7	Least Functionality	
	CM-9	Configuration Management Plan	
Contingency Planning	CP-1	Contingency Planning Policy and Procedures	
	CP-2	Contingency Plan	
	CP-3	Contingency Training	
	CP-4	Contingency Plan Testing and Exercises	
	CP-6	Alternate Storage Site	
	CP-7	Alternate Processing Site	
	CP-9	Information System Backup	
	CP-10	Information System Recovery and Reconstitution	
Identification and Authentication	IA-1	Identification and Authentication Policy and Procedures	
	IA-2	Identification and Authentication (Organizational Users)	
	IA-3	Device Identification and Authentication	
	IA-4	Identifier Management	
	IA-5	Authenticator Management	

CONTROL FAMILY	NUMBER	NIST SP 800-53 CONTROLS	POLICY SECTION(S)
	IA-6	Authenticator Feedback	
	IA-7	Cryptographic Module Authentication	
	IA-8	Identification and Authentication (Non-Organizational Users)	
Incident Response	IR-1	Incident Response Policy and Procedures	
	IR-2	Incident Response Training	
	IR-4	Incident Handling	
	IR-5	Incident Monitoring	
	IR-6	Incident Reporting	
	IR-7	Incident Response Assistance	
	IR-8	Incident Response Plan	
Maintenance	MA-1	System Maintenance Policy and Procedures	
	MA-3	Maintenance Tools	
	MA-4	Non-Local Maintenance	
	MA-5	Maintenance Personnel	
	MA-6	Timely Maintenance	
Media Protection	MP-1	Media Protection Policy and Procedures	
	MP-2	Media Access	
	MP-3	Media Marking	
	MP-4	Media Storage	
	MP-6	Media Sanitization	
Personnel Security	PS-1	Personnel Security Policy and Procedures	
	PS-2	Position Categorization	
	PS-3	Personnel Screening	
	PS-4	Personnel Termination	
	PS-5	Personnel Transfer	
	PS-6	Access Agreements	
	PS-7	Third-Party Personnel Security	
	PS-8	Personnel Sanctions	

CONTROL FAMILY	NUMBER	NIST SP 800-53 CONTROLS	POLICY SECTION(S)
Physical and Environmental Protection	PE-1	Physical and Environmental Protection Policy and Procedures	
	PE-3	Physical Access Control	
	PE-4	Access Control for Transmission Medium	
	PE-5	Access Control for Output Devices	
	PE-6	Monitoring Physical Access	
	PE-9	Power Equipment and Power Cabling	
	PE-11	Emergency Power	
	PE-13	Fire Protection	
	PE-14	Temperature and Humidity Controls	
	PE-15	Water Damage Protection	
	PE-16	Delivery and Removal	
	PE-17	Alternate Work Site	
	PE-18	Location of Information System Components	
PE-19	Information Leakage		
Planning	PL-1	Security Planning Policy and Procedures	
	PL-2	System Security Plan	
	PL-4	Rules of Behavior	
	PL-5	Privacy Impact Assessment	
	PL-6	Security-Related Activity Planning	
Program Management	PM-1	Information Security Program Plan	
	PM-2	Senior Information Security Officer	
	PM-3	Information Security Resources	
	PM-4	Plan of Action and Milestones Process	
	PM-6	Information Security Measures of Performance	

CONTROL FAMILY	NUMBER	NIST SP 800-53 CONTROLS	POLICY SECTION(S)
	PM-7	Enterprise Architecture	
	PM-8	Critical Infrastructure Plan	
	PM-9	Risk Management Strategy	
	PM-10	Security Authorization Process	
Risk Assessment	RA-1	Risk Assessment Policy and Procedures	
	RA-2	Security Categorization	
	RA-3	Risk Assessment	
	RA-5	Vulnerability Scanning	
Security Assessment and Authorization	CA-1	Security Assessment and Authorization Policies and Procedures	
	CA-2	Security Assessments	
	CA-3	Information System Connections	
	CA-6	Security Authorization	
	CA-7	Continuous Monitoring	
System and Communications Protection	SC-1	System and Communications Protection Policy and Procedures	
	SC-2	Application Partitioning	
	SC-4	Information In Shared Resources	
	SC-6	Resource Priority	
	SC-8	Transmission Integrity	
	SC-9	Transmission Confidentiality	
	SC-10	Network Disconnect	
	SC-11	Trusted Path	
	SC-12	Cryptographic Key Establishment and Management	
	SC-13	Use of Cryptography	
	SC-14	Public Access Protections	
	SC-15	Collaborative Computing Devices	
	SC-16	Transmission of Security Attributes	

CONTROL FAMILY	NUMBER	NIST SP 800-53 CONTROLS	POLICY SECTION(S)
	SC-17	Public Key Infrastructure Certificates	
	SC-18	Mobile Code	
	SC-28	Protection of Information at Rest	
	SC-29	Heterogeneity	
	SC-30	Virtualization Techniques	
	SC-31	Covert Channel Analysis	
	SC-33	Transmission Preparation Integrity	
	SC-34	Non-Modifiable Executable Programs	
System and Information Integrity	SI-1	System and Information Integrity Policy and Procedures	
	SI-2	Flaw Remediation	
	SI-3	Malicious Code Protection	
	SI-4	Information System Monitoring	
	SI-5	Security Alerts, Advisories, and Directives	
	SI-6	Security Functionality Verification	
	SI-7	Software and Information Integrity	
	SI-8	Spam Protection	
	SI-9	Information Input Restrictions	
	SI-10	Information Input Validation	
	SI-11	Error Handling	
	SI-12	Information Output Handling and Retention	
	SI-13	Predictable Failure Prevention	
System and Services Acquisition	SA-1	System and Services Acquisition Policy and Procedures	
	SA-2	Allocation of Resources	
	SA-3	Life Cycle Support	
	SA-4	Acquisitions	

CONTROL FAMILY	NUMBER	NIST SP 800-53 CONTROLS	POLICY SECTION(S)
	SA-5	Information System Documentation	
	SA-6	Software Usage Restrictions	
	SA-7	User-Installed Software	
	SA-8	Security Engineering Principles	
	SA-9	External Information System Services	
	SA-10	Developer Configuration Management	
	SA-11	Developer Security Testing	
	SA-12	Supply Chain Protections	
	SA-13	Trustworthiness	
	SA-14	Critical Information System Components	

APPENDIX E: LEGISLATIVE POLICY DRIVERS

Title	Description
HIPAA (Health Insurance Portability and Accountability Act of 1996): HIPAA Security Rule (2003)	The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) required the Department of Health and Human Services (HHS) to establish national standards for the security of electronic health care information. The final rule adopting HIPAA standards for security was published in the Federal Register on February 20, 2003. This final rule specifies a series of administrative, technical, and physical security procedures for covered entities to use to assure the confidentiality of electronic protected health information. The standards are delineated into either required or addressable implementation specifications.
California State Civil Code §1798.81	Protection and Disposal of Personal Information
California State Civil Code §1798.82	Disclosure of Security Breach involving Personal Information
California State Civil Code §1798.83	Disclosure of Personal Information to Third-parties
California State Civil Code §1798.84	Explains violations of civil codes §1798.81 - 1798.84
California Senate Bill 1386 (2002)	Amended civil code §1798.82, §1798.84, and added California Notice of Security Breach Law (civil code §1798.29)
California Assembly Bill 1298 (2007)	Amended civil code §1798.29 & §1798.82, to include medical information as personal information

APPENDIX F: EMPLOYEE ACKNOWLEDGEMENT

By signing this document, I acknowledge that I have read, understand, and shall abide by the County of Orange Cybersecurity Policy.

Employee Name (please print): _____

Employee Signature: _____

Department/Department: _____

Date: _____

CERTIFICATION OF RETURN OR DESTRUCTION AND NON-DATA BREACH

Upon the earlier of the closing of this project engagement, as a result of completion and/or other means, or the request (at any time) of County, Contractor shall (1) thoroughly complete the tables herein with information sufficient to allow the County to account for its documents, materials, and information and ensure their secure return or destruction; (2) at the County's option and pursuant to the County's written authorization: (a) return all copies of documents, materials, and information obtained from, or on behalf of, the County; and/or (b) securely destroy all documents, materials, and information obtained from, or on behalf of, the County; and (3) sign the certification below.

In the event Contractor returns documents, materials, and information to the County, the Contractor shall thoroughly complete the following table (including additional lines as needed):

Contractor	Project	What was supplied to the Contractor and Date	What was returned to the County and Date

In the event the County authorizes certain documents, materials, and information not to be returned to the County and authorized their destruction, Contractor shall securely destroy the residual data in accordance with secure destruction NIST Special Publication 800-88 Revision I (or the most current version) or a documented manner acceptable to the County Chief Security Officer and thoroughly complete the following table (including additional lines as needed):

Contractor	Project	Unique Certificate Number	What was securely destroyed?	When it was securely destroyed?

Attachment F

The undersigned hereby certifies that Contractor has returned or securely destroyed all copies of documents and materials provided to it by, or on behalf of, the County of Orange, as described on the attached Receipt Acknowledgements, other than those documents and materials listed in Attachment A to this certification. The undersigned further certifies that there have been no known or suspected data breaches pertaining to the documents and materials described on the attached Receipt Acknowledgments while they were in the possession, custody or control of *TBD/Selected Contractor* and its approved Affiliates, if any.

CONTRACTOR/TBD for itself and each of its Affiliates and subsidiaries

Name: _____

Title: _____

Signature: _____

Date: _____

DRUG FREE WORKPLACE CERTIFICATION

Orange County Human Relations Council

Company/Organization Name

The Contractor or grant recipient named above hereby certifies compliance with Government Code 8355 in matters relating to providing a drug-free workplace. The above named Contractor will:

1. Publish a statement notifying employees that unlawful manufacture, distribution, dispensation, possession, or use of a controlled substance is prohibited in the person's or organization's workplace and specifying the actions to be taken against employees for violations of the prohibitions, as required by Government Code Section 8355(a).
2. Establish a Drug Free Awareness Program as required by Government Code Section 8355(b), to inform employees about all of the following:
 - A. The dangers of drug abuse in the workplace,
 - B. The person's or organization's policy of maintaining a drug-free workplace,
 - C. Any available drug counseling, rehabilitation and employee assistance programs, and
 - D. Penalties that may be imposed upon employees for drug abuse violations
3. Provide as required by Government code Section 8355I that every employee who works on the proposed contract or grant:
 - A. Will receive a copy of the company's drug-free policy statement described in paragraph (1) above, and
 - B. Will agree to abide by the terms of the company's statement as a condition of employment in the contract or grant.

CERTIFICATION

I, the official named below, hereby swear that I am duly authorized legally to bind the Contractor or grant recipient to the above described certification.

Alison Edwards

Official's Name

11/10/2022

Orange

Date Executed
Alison Edwards

Executed in the County of Orange

E72E8BDFED364C7...

CEO

Contractor or Grantee Recipient Signature and Title

Exhibit 2

**CERTIFICATION REGARDING
DEBARMENT, SUSPENSION, INELIGIBILITY AND VOLUNTARY EXCLUSION
LOWER TIER COVERED TRANSACTIONS**

This certification is required by the regulations implementing Executive Order 12549, Debarment and suspension, 29 CFR Part 98.510, Participants' responsibilities. The regulations were published as Part VII of the May 26, 1988 Federal Register (pages 19160-19211)

(BEFORE COMPLETING CERTIFICATION, READ INSTRUCTIONS FOR CERTIFICATION)

- (1) The Contractor or grant recipient of Federal assistance funds certifies, by submission of this exhibit document, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any Federal department or agency.
- (2) Where the Contractor or grant recipient of Federal assistance funds is unable to certify to any of the statements in this certification, the Contractor or grant recipient shall attach an explanation to this exhibit document.

Alison Edwards

Name

CEO

Title

DocuSigned by:

Alison Edwards

11/10/2022

BT2E8BDFFD36407

Authorized Signature

Date

Exhibit 2**DEBARMENT AND SUSPENSION CERTIFICATION - Instructions for Certification**

1. By signing and submitting this exhibit document, the Contractor or grant recipient of Federal assistance funds is providing the certification as set out below.
2. The certification in the clause is a material representation of fact upon which reliance was placed when this transaction was entered into. If it is later determined that the Contractor or grant recipient of Federal assistance funds knowingly rendered an erroneous certification in addition to other remedies available to the Federal Government, the Department of Labor (DOL) may pursue available remedies, including suspension and/or debarment.
3. The Contractor recipient of Federal assistance funds shall provide immediate written notice to the County of Orange/Workforce Investment Board to which this certification document is submitted if at any time the Contractor or grant recipient of Federal assistance funds learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.
4. The Contractor or grant recipient of Federal assistance funds agrees by submitting this certification document that, should the covered transaction be entered into, it shall not knowingly enter into any lower tier covered transaction with a person who is debarred, suspended, declared ineligible, or voluntarily excluded from participation in this covered transaction, unless authorized by the DOL.
5. The Contractor or grant recipient of Federal assistance funds further agrees by submitting this certification document that it will include the clause titled "Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion - Lower Tier Covered Transactions," without modification, in all lower tier covered transactions and in all solicitations for lower tier covered transactions.
6. The Contractor or grant recipient in a covered transaction may rely upon a certification of a Contractor or grant recipient in a lower tier covered transaction that it is not debarred, suspended, ineligible, or voluntarily excluded from the covered transaction, unless it knows that the certification is erroneous. The Contractor or grant recipient may decide the method and frequency by which it determines the eligibility of its principals.
7. Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render in good faith the certification required by this clause. The knowledge and information of the Contractor or grant recipient is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.
8. Except for transactions authorized under paragraph 5 of these instructions, if the Contractor or grant recipient in a covered transaction knowingly enters into a lower tier covered transaction with a person who is suspended, debarred, ineligible, or voluntarily excluded from participation in this transaction, in addition to other remedies available to the Federal Government, the DOL may pursue available remedies, including suspension and/or debarment.

**CERTIFICATION REGARDING LOBBYING
CERTIFICATION FOR CONTRACTS, GRANTS, LOANS,
AND COOPERATIVE AGREEMENTS**

The undersigned certifies, to the best of his or her knowledge and belief, that:

- (1) No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.
- (2) If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.
- (3) The undersigned shall require that the language of this certification be included in the award documents for all* subawards at all tiers (including subcontracts, subgrants and contracts under grants, loans, and cooperative agreements) and that all* Contractors shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by section 1352, title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than \$10, 000 and not more than \$100,000 for each such failure.

Orange County Human Relations Council

Grantee/Contractor Organization

Alison Edwards

Name

CEO

Title

Alison Edwards

Authorized Signature

*Note: In these instances, "All," in the Final Rule is expected to be clarified to show that it applies to covered contract/grant transactions over \$100,000 (per OMB).

Exhibit 4**INSTRUCTIONS FOR COMPLETION OF
SF-LLL DISCLOSURE OF LOBBYING ACTIVITIES**

This disclosure form shall be completed by the reporting entity, whether subawardee or prime Federal recipient at the initiation or receipt of a covered Federal action, or a material change to a previous filing, pursuant to title 31 U.S.C. section 1352. The filing of a form is required for each payment or agreement to make payment to any lobbying entity for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with a covered Federal action. Use the SF LLL-A Continuation sheet for additional information if the space on the form is inadequate. Complete all items that apply for both the initial filing and material change report. Refer to the implementing guidance published by the Office of Management and Budget for additional information.

1. Identify the type of covered Federal action for which lobbying is and has been secured to influence the outcome of a covered action.
2. Identify the status of the covered Federal action.
3. Identify the appropriate classification of this report. If this is a follow up report caused by a material change to the information previously reported, enter the year and quarter in which the change occurred. Enter the date of the last previously submitted report by this reporting entity for this covered Federal action.
4. Enter the full name, address, city, state and zip code of the reporting entity. Include congressional district, if known. Check the appropriate classification of the reporting entity that designates if it is, or expects to be a prime or subaward recipient. Identify the tier of the subawardee, e. g. the first subawardee of the prime is the 1st tier. Subawards include but are not limited to subcontracts, subgrants and contract awards under grants.
5. If the organization filing the report, in item 4 checks "Subawardee", then enter the full name, address, city, state, and zip code of the prime Federal recipient. Include congressional district, if known.
6. Enter the name of the Federal agency making the award or loan commitment. Include at least one organizational level below agency name, if known. For example, Department of Transportation, United States Coast Guard.
7. Enter the Federal program name or description for the covered Federal action (item 1). If known, enter the full Catalog of Federal Domestic Assistance (CFDA) number for grants, cooperative agreements, loans and loan commitments.
8. Enter the most appropriate Federal identifying number available for the Federal action identified in item 1 (e. g. Request for Proposal (RFP) number; Invitation for Bid (IFB) number; grant announcement number the contract, grant, or loan award number; the application proposal control number assigned by the Federal agency). Include prefixes, e.g., "RFP DE 90 09."
9. For a covered Federal action where there has been an award or loan commitment by the Federal agency, enter the Federal amount of the award/loan commitment for the primary entity identified in item 4 or 5.
10.
 - (a) Enter the full name, address, city, state and zip code of the lobbying entity engaged by the reporting entity identified in item 4 to influence the covered Federal action.
 - (b) Enter the full names of the individual(s) performing services, and include full address if different from 10 (a). Enter Last Name, First Name, and Middle Initial (MI).
11. Enter the amount of compensation paid or reasonably expected to be paid by the reporting entity (item 4) to the lobbying entity (item 10). Indicate whether the payment has been made (actual) or will be made (planned). Check all boxes that apply. If this is a material change report enter the cumulative amount of payment made or planned to be made.
12. Check the appropriate box(es). Check all boxes that apply. If payment is made through an in kind contribution, specify the nature and value of the in kind payment.
13. Check the appropriate box(es). Check all boxes that apply. If other, specify nature.
14. Provide a specific and detailed description of the services that the lobbyist has performed, or will be expected to perform, and the date(s) of any services rendered. Include all preparatory and related activity, not just time spent in actual contact with Federal officials. Identify the Federal official(s) or employee(s) contacted and the officer(s), employee(s), or Member(s) of Congress that were contacted.
15. Check whether or not a SF LLL A Continuation Sheet(s) is attached.
16. The certifying official shall sign and date the form, print his/her name, title, and telephone number.

Public reporting burden for this collection of information is estimated to average 30 minutes per response, including time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to the Office of Management and Budget. Paperwork Reduction Project (0348 0046) Washington D.C., 20503.

Exhibit 4

DISCLOSURE OF LOBBYING ACTIVITIES

Complete this form to disclose activities pursuant to 31 U.S.C 1352

<p>1. Type of Federal Actions:</p> <ul style="list-style-type: none"> a. contract b. grant c. cooperative agreement d. loan e. loan guarantee f. loan insurance 	<p>2. Status of Federal Actions:</p> <ul style="list-style-type: none"> a. bid/offer/application b. initial award c. post-award 	<p>3. Report Type:</p> <ul style="list-style-type: none"> a. initial filing b. material change <p>For material change only: Year: _____ Quarter: _____ Date of last report: _____</p>
<p>4. Name and Address of Reporting Entity Prime Subawardee</p> <p>Tier _____ if known</p> <p>Congressional District, if known: _____</p>		<p>5. If Reporting Entity in No. 4 is a Subawardee: Enter Name and Address of Prime:</p> <p>Congressional District, if known: _____</p>
<p>6. Federal Department / Agency:</p>	<p>7. Federal Program Name/Description</p>	
<p>8. Federal Action Number, if known:</p>	<p>9. Award Amount, if known: \$ _____</p>	
<p>10a. Name and Address of Lobbying Entity (if individual, last name, first name, MI):</p> <p>(attach Continuation Sheets SF-LLL-A, if necessary)</p>	<p>10b. Individual Performing Services (including address if different from No. 10a) (last name, first name, MI):</p>	
<p>11. Amount of Payment (check all that apply): \$ Actual _____ Planned _____</p>	<p>13. Type of Payment (check all that apply)</p> <ul style="list-style-type: none"> a. retainer b. one-time free c. commission d. contingent fee e. deferred f. other specify: _____ 	
<p>12. Form of Payment (check all that apply):</p> <ul style="list-style-type: none"> a. cash b. in-kind: specify: _____ <p>nature: _____ value: _____</p>		
<p>14. Enter Description of Services performed or to be Performed and date(s) of Service, including officer(s), employee(s), or Member(s) contacted, for Payment indicated on item 11:</p>		
<p>15. Continuation sheet(s) SF-LLL-A attached: <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p>		
<p>16. Information requested through this form authorized by Title 31 U.S.C. Section 1352. This disclosure of lobbying activities is a material representation of fact upon which reliance was placed by the tier above when this transaction was made or entered into. This disclosure is required pursuant to 31 U.S.C. 1352. This information will be reported to the Congress semiannually and will be available for public inspection. An person who fails to file the required disclosure shall be subject to a civil penalty of not less than \$10,000 and not more than \$100,000 for each such failure.</p>		<p>Disclosed by: <u>Alison Edwards</u></p> <p>Signature: _____ <small>E72E8BDFED384C7...</small></p> <p>Print Name: Alison Edwards</p> <p>Title: CEO</p> <p>Telephone No: _____</p> <p>Date: 11/10/2022</p>

Exhibit 4

**DISCLOSURE OF LOBBYING ACTIVITIES
CONTINUATION SHEET**

Approved by OMS - 0348-0046

Reporting Entity: _____

Page _____ of _____

BILLING CODES 3410-01 -C; 6450-01-C; 6890-01 ;6025-01-C; 7510-01-C , 35 1 0-FE-C; 8120-01 -C; 4710-24-C, 6116-01 -C,



**Subject: OC Community Resources
Contract Reimbursement Policy**

Effective: July 1, 2010
Revised: January 17, 2020

PURPOSE:

This policy contains updated fiscal documentation requirements for contract reimbursement for OC Community Services and OC Housing & Community Development. The procedures provide instructions for submitting reimbursement demand letter or invoice.

REFERENCES:

Executed County Board of Supervisors approved contract
Budget included in contract or presented as an attachment
48 CFR Part 31 Contract Cost Principles and Procedures
24 CFR Parts 85, 570.502, 570.201, 576.21, 576.51 and 576.61: For OC Housing & Community Development Contracts only.
2 CFR Part 200 Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (Uniform Guidance)

BACKGROUND:

The executed Board of Supervisors approved contract is the authorization for all aspects of payment, including the maximum amount to be paid, the payee, and the scope of services and work. Payments are made in strict accordance with the contract terms. Allowable costs are identified in referenced Uniform Guidance and Code of Federal Regulations (CFR).

ATTACHMENTS:

Reimbursement Policy Status Form (RPS-1)

POLICY:

Contractor is responsible for the submission of accurate claims. This reimbursement policy is intended to ensure that the Contractor is reimbursed based on the code or codes that correctly describe the services provided. This information is intended to serve only as a general reference resource regarding OC Community Services' and OC Housing & Community Development's reimbursement policy for the services described and is not intended to address every aspect of a reimbursement situation. Accordingly, OC Community Services and OC Housing & Community Development may use reasonable discretion in interpreting and applying this policy to services provided in a particular case. Other factors affecting reimbursement may supplement, modify or, in some cases, supersede this policy. These factors may include, but are not limited to: legislative mandates and County directives. OC Community Services and OC Housing & Community Development may modify this reimbursement policy at any time by publishing a new version of the policy. However, the information presented in this policy is accurate and current as of the date of publication.

Cost incurred by Contractor must be substantiated and incurred during the contract period. Total of all reimbursements cannot exceed the amount of the contract. Cost must be allowable under applicable Code of Federal Regulations (CFR) or Uniform Guidance. All supporting documentation for reimbursement must be submitted with demand letter or invoice. If contract

requires matching contribution, documentation substantiating contribution match must be submitted with demand letter or invoice.

At any time, based on County's business needs and/or Contractor's performance, the County may designate Contractor to submit abbreviated or comprehensive documentation, as identified in the respective sections. Upon designation, Contractor will be notified, in writing via Reimbursement Policy Status Form, of which requirements are in full force. When Contractor is required to submit comprehensive documentation, in addition to the items identified in the Abbreviated Documentation Requirements Section, Contractor must also provide the documentation identified in the Comprehensive Documentation Requirements Section.

PROCEDURES:

Abbreviated Documentation Requirements

Compile and submit:

1. Supporting documentation includes, but is not limited to:
 - a. General ledger/expense transaction report
 - b. Payroll register or labor distribution report
 - c. Payroll allocation plan
 - d. Personnel Documentation
 - e. Benefit plan and calculation of benefit
 - f. Employer-employee contract for non-customary benefits (if applicable)
 - g. Pre-approval documentation for equipment purchases equal to or greater than \$5,000
2. The following is required with the first month's invoice only:
 - a. Cost allocation plan for rent, utilities, etc.
 - b. Indirect rate approved by cognizant agency (if applicable)
3. Summary of leveraged resources (if applicable)
4. Demand letters must contain the following certification (if required by Contract):

"By signing this report, I certify to the best of my knowledge and belief that the report is true, complete, and accurate, and the expenditures, disbursements and cash receipts are for the purposes and objectives set forth in the terms and conditions of the Federal award. I am aware that any false, fictitious, or fraudulent information, or the omission of any material fact, may subject me to criminal, civil or administrative penalties for fraud, false statements, false claims or otherwise. (U.S. Code Title 18, Section 1001 and Title 31 Sections 3729-3730 and 3801-3812)"
5. Grantee Performance Report (if required by Contract)
6. Supporting documentation shall be on single-sided sheets
7. Please redact employees' Social Security Number from payroll reports
8. Demand letter or invoice, along with supporting documentation shall be submitted to:

OC Community Resources Accounting
601 N. Ross St., 6th Floor
Santa Ana, CA 92701

Comprehensive Documentation Requirements

In addition to abbreviated documentation, compile and submit:

9. Purchase orders, invoices, and receipts
10. Cashed checks
11. Check register
12. Consultant/sub-contractor invoices (with description of services)
13. Travel expense documentation: mileage reimbursement, hotel bill, meal reimbursement

ACTION:

Distribute this policy to all appropriate staff

INQUIRIES: Inquiries may be directed to OCCR Accounts Payable at: OCCRAccountsPayable@occr.ocgov.com



Reimbursement Policy Status Form

Per OC Community Resources Contract Reimbursement Policy, in regards to the Contract # listed herein, Contractor is designated with the Documentation Status of Abbreviated unless Comprehensive is checked below. If the contractor’s designation should change to Abbreviated, a new status form shall be approved. All related documentation requirements are in full force, until further notice.

Contractor: Orange County Human Relations Council

Effective Date: 12/14/2022

Contract #: MA-012-22011942

Documentation Status: **Abbreviated** **Comprehensive**

Program Authorization by:

Auditor Controller Authorization by:

[Click here to enter text.](#)

[Click here to enter text.](#)

Print Name

Print Name

Signed by: _____

Signed by: _____

Date: [Click here to enter text.](#)

Date: [Click here to enter text.](#)

Two signatures are required to implement the form.

Distribution:

- Contractor
- Auditor Controller
- Contract File
- Program File