

COUNTY OF MONTEREY STANDARD AGREEMENT

This **Agreement** is made by and between the County of Monterey, a political subdivision of the State of California (hereinafter “County”) and:

SolutionsWest

(hereinafter “CONTRACTOR”).

In consideration of the mutual covenants and conditions set forth in this Agreement, the parties agree as follows:

1.0 GENERAL DESCRIPTION:

The County hereby engages CONTRACTOR to perform, and CONTRACTOR hereby agrees to perform, the services described in **Exhibit A** in conformity with the terms of this Agreement. The goods and/or services are generally described as follows:

Provide: temporary Medi-Cal Support Services for the Department of Social Services

2.0 PAYMENT PROVISIONS:

County shall pay the CONTRACTOR in accordance with the payment provisions set forth in **Exhibit A**, subject to the limitations set forth in this Agreement. The total amount payable by County to CONTRACTOR under this Agreement shall not exceed the sum of: \$ 1,654,215.00

3.0 TERM OF AGREEMENT:

3.01 The term of this Agreement is from October 1, 2023 to September 30, 2024, unless sooner terminated pursuant to the terms of this Agreement. This Agreement is of no force or effect until signed by both CONTRACTOR and County and with County signing last, and **CONTRACTOR may not commence work before County signs this Agreement.**

3.02 The County reserves the right to cancel this Agreement, or any extension of this Agreement, without cause, with a thirty day (30) written notice, or with cause immediately.

4.0 SCOPE OF SERVICES AND ADDITIONAL PROVISIONS:

The following attached exhibits are incorporated herein by reference and constitute a part of this Agreement:

Exhibit A Scope of Services/Payment Provisions

Exhibit B Other: See page 11(a) for a list of Exhibits

5.0 PERFORMANCE STANDARDS:

- 5.01 CONTRACTOR warrants that CONTRACTOR and CONTRACTOR's agents, employees, and subcontractors performing services under this Agreement are specially trained, experienced, competent, and appropriately licensed to perform the work and deliver the services required under this Agreement and are not employees of the County, or immediate family of an employee of the County.
- 5.02 CONTRACTOR, its agents, employees, and subcontractors shall perform all work in a safe and skillful manner and in compliance with all applicable laws and regulations. All work performed under this Agreement that is required by law to be performed or supervised by licensed personnel shall be performed in accordance with such licensing requirements.
- 5.03 CONTRACTOR shall furnish, at its own expense, all materials, equipment, and personnel necessary to carry out the terms of this Agreement, except as otherwise specified in this Agreement. CONTRACTOR shall not use County premises, property (including equipment, instruments, or supplies) or personnel for any purpose other than in the performance of its obligations under this Agreement.

6.0 PAYMENT CONDITIONS:

- 6.01 Prices shall remain firm for the initial term of the Agreement and, thereafter, may be adjusted annually as provided in this paragraph. The County does not guarantee any minimum or maximum amount of dollars to be spent under this Agreement.
- 6.02 Negotiations for rate changes shall be commenced, by CONTRACTOR, a minimum of ninety days (90) prior to the expiration of the Agreement. Rate changes are not binding unless mutually agreed upon in writing by the County and the CONTRACTOR.
- 6.03 Invoice amounts shall be billed directly to the ordering department.
- 6.04 CONTRACTOR shall submit such invoice periodically or at the completion of services, but in any event, not later than 30 days after completion of services. The invoice shall set forth the amounts claimed by CONTRACTOR for the previous period, together with an itemized basis for the amounts claimed, and such other information pertinent to the invoice. The County shall certify the invoice, either in the requested amount or in such other amount as the County approves in conformity with this Agreement and shall promptly submit such invoice to the County Auditor-Controller for payment. The County Auditor-Controller shall pay the amount certified within 30 days of receiving the certified invoice.

7.0 TERMINATION:

- 7.01 During the term of this Agreement, the County may terminate the Agreement for any reason by giving written notice of termination to the CONTRACTOR at least thirty (30) days prior to the effective date of termination. Such notice shall set forth the effective date of termination. In the event of such termination, the amount payable under this Agreement shall be reduced in proportion to the services provided prior to the date of termination.

- 7.02 The County may cancel and terminate this Agreement for good cause effective immediately upon written notice to CONTRACTOR. "Good cause" includes the failure of CONTRACTOR to perform the required services at the time and in the manner provided under this Agreement. If County terminates this Agreement for good cause, the County may be relieved of the payment of any consideration to CONTRACTOR, and the County may proceed with the work in any manner, which County deems proper. The cost to the County shall be deducted from any sum due the CONTRACTOR under this Agreement.
- 7.03 The County's payments to CONTRACTOR under this Agreement are funded by local, state and federal governments. If funds from local, state and federal sources are not obtained and continued at a level sufficient to allow for the County's purchase of the indicated quantity of services, then the County may give written notice of this fact to CONTRACTOR, and the obligations of the parties under this Agreement shall terminate immediately, or on such date thereafter, as the County may specify in its notice, unless in the meanwhile the parties enter into a written amendment modifying this Agreement.

8.0 INDEMNIFICATION:

CONTRACTOR shall indemnify, defend, and hold harmless the County, its officers, agents, and employees, from and against any and all claims, liabilities, and losses whatsoever (including damages to property and injuries to or death of persons, court costs, and reasonable attorneys' fees) occurring or resulting to any and all persons, firms or corporations furnishing or supplying work, services, materials, or supplies in connection with the performance of this Agreement, and from any and all claims, liabilities, and losses occurring or resulting to any person, firm, or corporation for damage, injury, or death arising out of or connected with the CONTRACTOR's performance of this Agreement, unless such claims, liabilities, or losses arise out of the sole negligence or willful misconduct of the County. "CONTRACTOR's performance" includes CONTRACTOR's action or inaction and the action or inaction of CONTRACTOR's officers, employees, agents and subcontractors.

9.0 INSURANCE REQUIREMENTS:

- 9.01 **Evidence of Coverage:** Prior to commencement of this Agreement, the Contractor shall provide a "Certificate of Insurance" certifying that coverage as required herein has been obtained. Individual endorsements executed by the insurance carrier shall accompany the certificate. In addition, the Contractor upon request shall provide a certified copy of the policy or policies.

This verification of coverage shall be sent to the County's Contracts/Purchasing Department, unless otherwise directed. The Contractor shall not receive a "Notice to Proceed" with the work under this Agreement until it has obtained all insurance required and the County has approved such insurance. This approval of insurance shall neither relieve nor decrease the liability of the Contractor.

- 9.02 **Qualifying Insurers:** All coverage's, except surety, shall be issued by companies which hold a current policy holder's alphabetic and financial size category rating of not less than A- VII, according to the current Best's Key Rating Guide or a company of equal financial stability that is approved by the County's Purchasing Manager.

9.03 **Insurance Coverage Requirements:** Without limiting CONTRACTOR's duty to indemnify, CONTRACTOR shall maintain in effect throughout the term of this Agreement a policy or policies of insurance with the following minimum limits of liability:

Commercial General Liability Insurance: including but not limited to premises and operations, including coverage for Bodily Injury and Property Damage, Personal Injury, Contractual Liability, Broad form Property Damage, Independent Contractors, Products and Completed Operations, with a combined single limit for Bodily Injury and Property Damage of not less than \$1,000,000 per occurrence.

(Note: any proposed modifications to these general liability insurance requirements shall be attached as an Exhibit hereto, and the section(s) above that are proposed as not applicable shall be lined out in blue ink. All proposed modifications are subject to County approval.)

Requestor must check the appropriate Automobile Insurance Threshold:

Requestor must check the appropriate box.

Agreement Under \$100,000 Business Automobile Liability Insurance: covering all motor vehicles, including owned, leased, non-owned, and hired vehicles, used in providing services under this Agreement, with a combined single limit for Bodily Injury and Property Damage of not less than \$500,000 per occurrence.

Agreement Over \$100,000 Business Automobile Liability Insurance: covering all motor vehicles, including owned, leased, non-owned, and hired vehicles, used in providing services under this Agreement, with a combined single limit or Bodily Injury and Property Damage of not less than \$1,000,000 per occurrence.

(Note: any proposed modifications to these auto insurance requirements shall be attached as an Exhibit hereto, and the section(s) above that are proposed as not applicable shall be lined out in blue ink. All proposed modifications are subject to County approval.)

Workers' Compensation Insurance: if CONTRACTOR employs others in the performance of this Agreement, in accordance with California Labor Code section 3700 and with Employer's Liability limits not less than \$1,000,000 each person, \$1,000,000 each accident and \$1,000,000 each disease.

(Note: any proposed modifications to these workers' compensation insurance requirements shall be attached as an Exhibit hereto, and the section(s) above that are proposed as not applicable shall be lined out in blue ink. All proposed modifications are subject to County approval.)

Professional Liability Insurance: if required for the professional services being provided, (e.g., those persons authorized by a license to engage in a business or profession regulated by the California Business and Professions Code), in the amount of not less than \$1,000,000 per claim and \$2,000,000 in the aggregate, to cover liability for malpractice or errors or omissions made in the course of rendering professional services. If professional liability insurance is written on a "claims-made" basis rather than an occurrence basis, the CONTRACTOR shall, upon the expiration or earlier termination of this Agreement, obtain extended reporting coverage ("tail coverage") with the same liability limits. Any such tail

coverage shall continue for at least three years following the expiration or earlier termination of this Agreement.

(Note: any proposed modifications to these insurance requirements shall be attached as an Exhibit hereto, and the section(s) above that are proposed as not applicable shall be lined out in blue ink. All proposed modifications are subject to County approval.)

9.04 Other Requirements:

All insurance required by this Agreement shall be with a company acceptable to the County and issued and executed by an admitted insurer authorized to transact Insurance business in the State of California. Unless otherwise specified by this Agreement, all such insurance shall be written on an occurrence basis, or, if the policy is not written on an occurrence basis, such policy with the coverage required herein shall continue in effect for a period of three years following the date CONTRACTOR completes its performance of services under this Agreement.

Each liability policy shall provide that the County shall be given notice in writing at least thirty days in advance of any endorsed reduction in coverage or limit, cancellation, or intended non-renewal thereof. Each policy shall provide coverage for Contractor and additional insureds with respect to claims arising from each subcontractor, if any, performing work under this Agreement, or be accompanied by a certificate of insurance from each subcontractor showing each subcontractor has identical insurance coverage to the above requirements.

Commercial general liability and automobile liability policies shall provide an endorsement naming the County of Monterey, its officers, agents, and employees as Additional Insureds with respect to liability arising out of the CONTRACTOR'S work, including ongoing and completed operations, **and shall further provide that such insurance is primary insurance to any insurance or self-insurance maintained by the County and that the insurance of the Additional Insureds shall not be called upon to contribute to a loss covered by the CONTRACTOR'S insurance.** The required endorsement form for Commercial General Liability Additional Insured is ISO Form CG 20 10 11-85 or CG 20 10 10 01 in tandem with CG 20 37 10 01 (2000). The required endorsement form for Automobile Additional Insured endorsement is ISO Form CA 20 48 02 99.

Prior to the execution of this Agreement by the County, CONTRACTOR shall file certificates of insurance with the County's contract administrator and County's Contracts/Purchasing Division, showing that the CONTRACTOR has in effect the insurance required by this Agreement. The CONTRACTOR shall file a new or amended certificate of insurance within five calendar days after any change is made in any insurance policy, which would alter the information on the certificate then on file. Acceptance or approval of insurance shall in no way modify or change the indemnification clause in this Agreement, which shall continue in full force and effect. CONTRACTOR shall always during the term of this Agreement maintain in force the insurance coverage required under this Agreement and shall send, without demand by County, annual certificates to County's Contract Administrator and County's Contracts/Purchasing Division. If the certificate is not received by the expiration date, County shall notify CONTRACTOR and CONTRACTOR shall have five calendar days to send in the certificate, evidencing no lapse in coverage during the interim. Failure by CONTRACTOR to maintain such insurance is a default of

this Agreement, which entitles County, at its sole discretion, to terminate this Agreement immediately.

10.0 RECORDS AND CONFIDENTIALITY:

- 10.1 **Confidentiality:** CONTRACTOR and its officers, employees, agents, and subcontractors shall comply with any and all federal, state, and local laws, which provide for the confidentiality of records and other information. CONTRACTOR shall not disclose any confidential records or other confidential information received from the County or prepared in connection with the performance of this Agreement, unless County specifically permits CONTRACTOR to disclose such records or information. CONTRACTOR shall promptly transmit to County any and all requests for disclosure of any such confidential records or information. CONTRACTOR shall not use any confidential information gained by CONTRACTOR in the performance of this Agreement except for the sole purpose of carrying out CONTRACTOR's obligations under this Agreement.
- 10.2 **County Records:** When this Agreement expires or terminates, CONTRACTOR shall return to County any County records which CONTRACTOR used or received from County to perform services under this Agreement.
- 10.3 **Maintenance of Records:** CONTRACTOR shall prepare, maintain, and preserve all reports and records that may be required by federal, state, and County rules and regulations related to services performed under this Agreement. CONTRACTOR shall maintain such records for a period of at least three years after receipt of final payment under this Agreement. If any litigation, claim, negotiation, audit exception, or other action relating to this Agreement is pending at the end of the three-year period, then CONTRACTOR shall retain said records until such action is resolved.
- 10.4 **Access to and Audit of Records:** The County shall have the right to examine, monitor and audit all records, documents, conditions, and activities of the CONTRACTOR and its subcontractors related to services provided under this Agreement. Pursuant to Government Code section 8546.7, if this Agreement involves the expenditure of public funds in excess of \$10,000, the parties to this Agreement may be subject, at the request of the County or as part of any audit of the County, to the examination and audit of the State Auditor pertaining to matters connected with the performance of this Agreement for a period of three years after final payment under the Agreement.
- 10.5 **Royalties and Inventions:** County shall have a royalty-free, exclusive and irrevocable license to reproduce, publish, and use, and authorize others to do so, all original computer programs, writings, sound recordings, pictorial reproductions, drawings, and other works of similar nature produced in the course of or under this Agreement. CONTRACTOR shall not publish any such material without the prior written approval of County.

11.0 NON-DISCRIMINATION:

- 11.1 During the performance of this Agreement, CONTRACTOR, and its subcontractors, shall not unlawfully discriminate against any person because of race, religious creed, color, sex, national origin, ancestry, physical disability, mental disability, medical condition, marital status, age (over 40), sexual orientation, or any other characteristic set forth in California Government code § 12940(a), either in CONTRACTOR's employment practices or in the furnishing of services to recipients. CONTRACTOR shall ensure that the evaluation and

treatment of its employees and applicants for employment and all persons receiving and requesting services are free of such discrimination. CONTRACTOR and any subcontractor shall, in the performance of this Agreement, fully comply with all federal, state, and local laws and regulations which prohibit discrimination. The provision of services primarily or exclusively to such target population as may be designated in this Agreement shall not be deemed to be prohibited discrimination.

12.0 COMPLIANCE WITH TERMS OF STATE OR FEDERAL GRANTS:

If this Agreement has been or will be funded with monies received by the County pursuant to a contract with the state or federal government in which the County is the grantee, CONTRACTOR will comply with all the provisions of said contract, to the extent applicable to CONTRACTOR as a subgrantee under said contract, and said provisions shall be deemed a part of this Agreement, as though fully set forth herein. Upon request, County will deliver a copy of said contract to CONTRACTOR, at no cost to CONTRACTOR.

13.0 COMPLIANCE WITH APPLICABLE LAWS:

13.1 CONTRACTOR shall keep itself informed of and in compliance with all federal, state, and local laws, ordinances, regulations, and orders, including but not limited to all state and federal tax laws that may affect in any manner the Project or the performance of the Services or those engaged to perform Services under this AGREEMENT as well as any privacy laws including, if applicable, HIPAA. CONTRACTOR shall procure all permits and licenses, pay all charges and fees, and give all notices require by law in the performance of the Services.

13.2 CONTRACTOR shall report immediately to County's Contracts/Purchasing Officer, in writing, any discrepancy or inconsistency it discovers in the laws, ordinances, regulations, orders, and/or guidelines in relation to the Project of the performance of the Services.

13.3 All documentation prepared by CONTRACTOR shall provide for a completed project that conforms to all applicable codes, rules, regulations, and guidelines that are in force at the time such documentation is prepared.

14.0 INDEPENDENT CONTRACTOR:

In the performance of work, duties, and obligations under this Agreement, CONTRACTOR is always acting and performing as an independent contractor and not as an employee of the County. No offer or obligation of permanent employment with the County or County department or agency is intended in any manner, and CONTRACTOR shall not become entitled by virtue of this Agreement to receive from County any form of employee benefits including but not limited to sick leave, vacation, retirement benefits, workers' compensation coverage, insurance or disability benefits. CONTRACTOR shall be solely liable for and obligated to pay directly all applicable taxes, including federal and state income taxes and social security, arising out of CONTRACTOR's performance of this Agreement. In connection therewith, CONTRACTOR shall defend, indemnify, and hold County harmless from any and all liability which County may incur because of CONTRACTOR's failure to pay such taxes.

15.0 NOTICES:

Notices required under this Agreement shall be delivered personally or by first-class, postage pre-paid mail to the County and CONTRACTOR'S contract administrators at the addresses listed below:

FOR COUNTY:	FOR CONTRACTOR:
Lori A. Medina, Director	Renee Carter, President/CEO
Name and Title	Name and Title
1000 S. Main St., Suite 301, Salinas, CA 93901	1725 10th Street, Suite 201, Sacramento, CA 95811
Address	Address
831-755-4430	916-765-7886
Phone:	Phone:

16.0 MISCELLANEOUS PROVISIONS.

- 16.01 **Conflict of Interest:** CONTRACTOR represents that it presently has no interest and agrees not to acquire any interest during the term of this Agreement, which would directly, or indirectly conflict in any manner or to any degree with the full and complete performance of the services required to be rendered under this Agreement.
- 16.02 **Amendment:** This Agreement may be amended or modified only by an instrument in writing signed by the County and the CONTRACTOR.
- 16.03 **Waiver:** Any waiver of any terms and conditions of this Agreement must be in writing and signed by the County and the CONTRACTOR. A waiver of any of the terms and conditions of this Agreement shall not be construed as a waiver of any other terms or conditions in this Agreement.
- 16.04 **Contractor:** The term "CONTRACTOR" as used in this Agreement includes CONTRACTOR's officers, agents, and employees acting on CONTRACTOR's behalf in the performance of this Agreement.
- 16.05 **Disputes:** CONTRACTOR shall continue to perform under this Agreement during any dispute.
- 16.06 **Assignment and Subcontracting:** The CONTRACTOR shall not assign, sell, or otherwise transfer its interest or obligations in this Agreement without the prior written consent of the County. None of the services covered by this Agreement shall be subcontracted without the prior written approval of the County. Notwithstanding any such subcontract, CONTRACTOR shall continue to be liable for the performance of all requirements of this Agreement.

- 16.07 **Successors and Assigns:** This Agreement and the rights, privileges, duties, and obligations of the County and CONTRACTOR under this Agreement, to the extent assignable or delegable, shall be binding upon and inure to the benefit of the parties and their respective successors, permitted assigns, and heirs.
- 16.08 **Headings:** The headings are for convenience only and shall not be used to interpret the terms of this Agreement.
- 16.09 **Time is of the Essence:** Time is of the essence in each and all of the provisions of this Agreement.
- 16.10 **Governing Law:** This Agreement shall be governed by and interpreted under the laws of the State of California; venue shall be Monterey County.
- 16.11 **Non-exclusive Agreement:** This Agreement is non-exclusive and both County and CONTRACTOR expressly reserve the right to contract with other entities for the same or similar services.
- 16.12 **Construction of Agreement:** The County and CONTRACTOR agree that each party has fully participated in the review and revision of this Agreement and that any rule of construction to the effect that ambiguities are to be resolved against the drafting party shall not apply in the interpretation of this Agreement or any amendment to this Agreement.
- 16.13 **Counterparts:** This Agreement may be executed in two or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same Agreement.
- 16.14 **Authority:** Any individual executing this Agreement on behalf of the County or the CONTRACTOR represents and warrants hereby that he or she has the requisite authority to enter into this Agreement on behalf of such party and bind the party to the terms and conditions of this Agreement.
- 16.15 **Integration:** This Agreement, including the exhibits, represent the entire Agreement between the County and the CONTRACTOR with respect to the subject matter of this Agreement and shall supersede all prior negotiations, representations, or agreements, either written or oral, between the County and the CONTRACTOR as of the effective date of this Agreement, which is the date that the County signs the Agreement.
- 16.16 **Interpretation of Conflicting Provisions:** In the event of any conflict or inconsistency between the provisions of this Agreement and the Provisions of any exhibit or other attachment to this Agreement, the provisions of this Agreement shall prevail and control.

17.0 **CONSENT TO USE OF ELECTRONIC SIGNATURES.**

- 17.1 The parties to this Agreement consent to the use of electronic signatures via DocuSign to execute this Agreement. The parties understand and agree that the legality of electronic signatures is governed by state and federal law, 15 U.S.C. Section 7001 et seq.; California Government Code Section 16.5; and, California Civil Code Section 1633.1 et. seq. Pursuant to said state and federal law as may be amended from time to time, the parties to this Agreement hereby authenticate and execute this Agreement, and any and all Exhibits to this

Agreement, with their respective electronic signatures, including any and all scanned signatures in portable document format (PDF).

17.2 Counterparts.

The parties to this Agreement understand and agree that this Agreement can be executed in two (2) or more counterparts and transmitted electronically via facsimile transmission or by delivery of a scanned counterpart in portable document format (PDF) via email transmittal.

17.3 Form: Delivery by E-Mail or Facsimile.

Executed counterparts of this Agreement may be delivered by facsimile transmission or by delivery of a scanned counterpart in portable document format (PDF) by e-mail transmittal, in either case with delivery confirmed. On such confirmed delivery, the signatures in the facsimile or PDF data file shall be deemed to have the same force and effect as if the manually signed counterpart or counterparts had been delivered to the other party in person.

***** THIS SECTION INTENTIONALLY LEFT BLANK *****

18.0 SIGNATURE PAGE.

IN WITNESS WHEREOF, County and CONTRACTOR have executed this Agreement as of the day and year written below.

COUNTY OF MONTEREY

CONTRACTOR

By: _____
Contracts/Purchasing Officer

Date: _____

By: _____
Department Head (if applicable)

Date: _____

Approved as to Form
County Counsel
Leslie J. Girard, County Counsel

By: DocuSigned by:
Anne Brenton

Office of the County Counsel

Date: 8/30/2023 | 1:38 PM PDT

Approved as to Fiscal Provisions

By: DocuSigned by:
Patricia Ruiz

Auditor/Controller

Date: 8/31/2023 | 7:40 AM PDT

By: _____
Risk Management

Date: _____

SolutionsWest

Contractor/Business Name *

By: DocuSigned by:
Renee Carter

F91246 (Signature of Chair, President, or Vice-President)

Renee Carter

Name and Title

Date: 8/30/2023 | 10:08 AM PDT

By: _____
(Signature of Secretary, Asst. Secretary, CFO, Treasurer, or
Asst. Treasurer)

Name and Title

Date: _____

County Board of Supervisors' Agreement No. _____ approved on _____

*INSTRUCTIONS: If CONTRACTOR is a corporation, including non-profit corporations, the full legal name of the corporation shall be set forth above together with the signatures of two (2) specified officers per California Corporations Code Section 313. If CONTRACTOR is a Limited Liability Corporation (LLC), the full legal name of the LLC shall be set forth above together with the signatures of two (2) managers. If CONTRACTOR is a partnership, the full legal name of the partnership shall be set forth above together with the signature of a partner who has authority to execute this Agreement on behalf of the partnership. If CONTRACTOR is contracting in an individual capacity, the individual shall set forth the name of the business, if any, and shall personally sign the Agreement or Amendment to said Agreement.

¹Approval by County Counsel is required

²Approval by Auditor-Controller is required

³Approval by Risk Management is necessary only if changes are made in paragraphs 8 or 9

LIST OF EXHIBITS
SolutionsWest

Exhibit A	Scope of Services
Exhibit B	DSS Additional Provisions
Exhibit C	Budget
Exhibit D	Invoice
Exhibit E	Weekly Status Report
Exhibit F	MCDSS Onboarding
Exhibit G	Lobbying Certification
Exhibit H	Child Abuse & Neglect Reporting Certification
Exhibit I	Elder Abuse & Neglect Reporting Certification

SOLUTIONS WEST

Scope of Services/Payment Provisions

October 1, 2023 – September 30, 2024

I. CONTACTS

a. Primary Contacts

<i>County</i>	<i>Contractor</i>
Aaron McDougal Management Analyst II Department of Social Services 713 La Guardia, Suite A Salinas, CA 93905 Phone: (831) 796-3577 McDougalAD@co.monterey.ca.us	Cale Bryan Managing Director SolutionsWest 1725 10 th Street, Suite 201 Sacramento, CA 95811 Phone: (916) 342-8231 Cbryan@solutionswest.com

b. Additional Contacts:

Rose DeFranco Deputy Director Department of Social Services 1000 South Main Street, Suite 211A Salinas, CA 93901 Phone: (831) 755-4403 Defrancor@co.monterey.ca.us	Renee Carter President/CEO SolutionsWest 1725 10 th Street, Suite 201 Sacramento, CA 95811 Phone: (916) 765-7886 Rcarter@solutionswest.com
---	--

II. BACKGROUND

Medi-Cal policy changes and seasonal demand for county services present resource challenges for MCDSS (Monterey County Department of Social Services) in 2023 and 2024. With the end of Medi-Cal Continuous Coverage on March 31, 2023, the MCDSS Community Benefits division is responsible for processing Medi-Cal renewals for the first time since 2020. Renewal activities started on April 1, 2023, for Medi-Cal participants with a June 2023 renewal date which includes processing negative actions such as increased share of cost determinations and discontinuance actions due to changes in eligibility and/or failure to provide verification. MCDSS has 14 months to complete renewals, returning to normal Medi-Cal redetermination operations by June of 2024, per the California Department of Healthcare Services (DHCS). Responding to the significant operational challenges associated with redetermining the eligibility of

all those on the MCDSS Medi-Cal rolls while managing staff vacancies, increased Medi-Cal caseload from 2020 to 2023 of 13% and the increase in demand for other services with Community Benefits requires assistance from a vendor that understands the Medi-Cal program and the data systems that support it.

To temporarily increase MCDSS capacity through the Medi-Cal unwinding and seasonal demand increase periods, Contractor can quickly mobilize and adjust to County specific procedures to immediately assist with data entry and case follow-up activities, resulting in timely and accurate client benefits during the 14 months Medi-Cal unwinding and season demand increase period. The Contractor team will not be making eligibility determinations or issuing benefits. These services are being provided on a limited basis to address the surge in demand, they are not replacing existing staff positions or intended to be a long-term resourcing strategy.

Contractor has conducted similar Medi-Cal support projects in California. In fact, Contractor worked with Monterey County DSS in a similar manner between 2014 and 2019. Additionally, Contractor has worked on Medi-Cal staffing projects with Mendocino County Social Services, Riverside County Department of Public Social Services, and most recently, San Benito County Health and Human Services Agency. Contractor supported thousands of Medi-Cal cases through these engagements.

Contractor is ideally suited to assist Monterey County DSS, given our experience in similar projects, staff qualifications, and subject matter expertise. The Contractor team includes former county staff with decades of experience providing client services for various programs such as Medi-Cal, CalFresh, CalWORKs, and General Assistance. Additionally, Contractor is conducting system training for all CalWIN counties migrating to CalSAWS in 2022 and 2023, so there is a depth of knowledge of the primary data system used for Medi-Cal services.

III. SERVICES TO BE PROVIDED

A. Medi-Cal Support Services/ Contractor Responsibilities

Contractor shall provide a Medi-Cal Support Services team consisting of 13 members, including 10 Support Specialists, 2 Supervisors, and 1 Project Manager.

Support Specialists: Support Specialist's will provide Medi-Cal processing assistance through a variety of actions. This will include reviewing Intake and Renewal packets, contacting clients to complete phone interviews, sending the appropriate form(s) requesting additional verification(s) as required by program/county policy and updating data collection pages in CalSAWS.

Supervisor: The Supervisor will provide oversight and conduct case quality reviews for 100% of cases assigned. They will also provide policy and process guidance to Support Specialists.

Project Manager: The Project Manager provides daily administrative and executive oversight of the project team. The Project Manager will be responsible for

maintaining quality and consistent communication of project deliverables to the DSS leadership team.

Contractor will conduct the project remotely, and will provide the following services to complete the project successfully:

1. Support Specialists, Supervisors, and the Project Manager will conduct all onboarding and support services remotely outside of the initial week of onsite onboarding.
2. Participate in a week-long onsite project orientation, hosted by DSS.
3. Supervisors will provide oversight of the Support Specialist team, distribute work, and conduct quality reviews.
4. Supervisors will deliver Weekly Productivity Reports that include: a. Cases reviewed b. Hours expended c. Issues, risks, and any other items deemed necessary.
5. Support Specialists will:
 - a. Review and provide the appropriate updates for Medi-Cal Intake applications and Renewals (redeterminations). Intake cases are the priority for Contractor, with additionally capacity dedicated to Renewals.
 - b. With the appropriate connectivity, image client verification documents through virtual print and index documents/verifications received as appropriate per county policy.
 - c. Process system tasks including, but not limited to, sending first or second requests for documents/verifications, request MAGI, monitor pending due dates, updating Applicant/Recipient Income and Eligibility Verification System (IEVS) reports, updating data related to address change, age change, income change, change reported, Medi-Cal 355 form, Renewal reports, Other Health Coverage (OHC) change, and conducting phone interviews with customers directly.
 - d. Contact customers as needed to obtain necessary documentation and to clarify information to complete the work assigned.
 - e. Entering all required journal records on all actions performed. For Intake and Renewals, once all information is input and the case is ready for EDBC actions, the Pending Authorization process will be utilized for a DSS Intake Supervisor to review and approve the EDBC results submitted by the Support Specialist. Note that the Contractor Supervisors will review case action before the case is sent to the DSS Supervisor for approval of EDBC results.
6. The Project Manager will:
 - a. Provide daily operational oversight of all Support Specialist & Supervisor activities.
 - b. Serve as an escalation point to Contractor Supervisors and MCDSS leadership.
 - c. Interface with MCDSS leadership on items including, but not limited to, work quality, policy, productivity, budget, and resource staffing.
7. Confidentiality
 - a. Each Contractor project team member will sign and comply with the terms of the Monterey County DSS Confidentiality Agreement.

b. The Contractor project team will oversee that work and documents remain secure and compliant with Personal Identification Information (PII) requirements.

8. If a resource departs voluntarily or for involuntary reasons, Contractor will assign a new resource with Medi-Cal experience. The assigned Supervisor is responsible for training the replacement resource on County-specific policies and procedures.

9. Contractor will be responsible at Contractors expense to return any County equipment, including but not limited to laptops, to County at the conclusion of contract, or at such time equipment is no longer required by Contractor.

B. County Project Responsibilities

Monterey County Department of Social Services will provide the project personnel, devices, data system credentials, and appropriate oversight to complete the project successfully.

MCDSS responsibilities include:

1. Hosting and facilitating one (1) week of dedicated training and onboarding for the Contractor Project team, led by MCDSS subject matter experts, at MCDSS facilities. The focus of this training is on current County specific business processes and policies that relate to the Medi-Cal program.
2. Provisioning laptops and zoom phone that can securely access the MCDSS network, and all systems required – CalSAWS, CalHEERS, MEDS.
3. Establishing a program and technical single point of contact for Contractor Project Manager and Supervisors.
4. Providing county specific policy guidance and escalations.
5. Distributing case assignments as needed. The MCDSS Clerical unit will link the CalHEERS MC Referrals and closed Determination Changes and assign into a separate caseload for Contractor staff to pull on a daily basis. Medi-Cal Renewals that are assigned will be transferred to a CalSAWS caseload built for Solutions West where they will be worked on, monitored when determined incomplete and fully processed within 5 days of the MC355 due date.
6. Reviewing and authorizing final Medi-Cal eligibility determinations using the Pending Authorization (first level authorization) process in CalSAWS.
7. Establishing remote sign-on access to California State Automated Welfare System (CalSAWS), Medi-Cal Eligibility Data Systems (MEDS), and California Healthcare Eligibility, Enrollment, and Retention System (CalHEERS) for all assigned staff.
8. Receiving and reviewing Weekly Productivity Reports and, as needed, remove barriers to completing scheduled events.

C. Payment Schedule:

Contractor proposes an all-inclusive hourly service fee by resource type, with a total maximum contract value for this engagement not-to-exceed One-Million Six Hundred Fifty-Four Thousand, Two-Hundred Fifteen dollars (\$1,654,215.00). Payment for services will be invoiced monthly for actual hours worked within thirty (30) days of the services provided. Fixed price One-Time Travel Costs will

be invoiced the month immediately following week-long onsite onboarding. Allowable costs for travel expenses incurred while providing services under this Agreement, must follow the Monterey County Auditor/Controller's Travel Policy www.co.monterey.ca.us/government/departments-a-h/auditor-controller/policies-and-procedures and must provide back-up documentation.

FY 2023/2024		Total	
Activity	Hours	Rate	Cost
1 Project Manager	1,944	\$81/hour	\$157,464
2 Supervisors	3,888	\$67/hour	\$260,496
10 Support Specialists	19,440	\$62.50/hour	\$1,215,000
One Time Travel Cost	N/A	N/A	\$21,255
			\$1,654,215

D. Staffing Requirements-Hiring

- a) Contractor agrees to conduct a pre-employment screening to determine appropriateness of the Contracted Employee for this assignment.
- b) Contractor agrees that all personnel assigned to this contract will be knowledgeable of Medi-Cal program requirements, the CalSAWS system, and qualified to provide Medi-Cal support services in the state of California.
- c) Contractor Employees should be acceptable to the County and available for the entire length of the assignment, however, if a replacement is required, a qualified replacement will be provided by the Contractor.
- d) The County reserves the right to require the replacement of any Contractor Employee. If for any reason, a replacement is required within the first eight (8) hours of service, there will be no charge to the County.
- e) The Contractor agrees to replace any Contractor Employee determined to be unsatisfactory.
- f) If at any time beyond the initial eight (8) hours of service, the Contractor Employee is determined to be unsatisfactory, the Contractor will only invoice for services up to the point the County contact notifies the Contractor that replacement must be made.
- g) Contractor Employees are solely the employees of the Contractor.

E. Staffing Requirements-

- a) It is expected Contractor will have a minimum of one (1) Supervisor and seven (7) Medi-Cal Support Specialists on duty each workday.
- b) Contractor will inform County contact on any workday Contractor will have fewer than seven (7) Medi-Cal Support Specialists, or less than one (1) Supervisor reporting for duty.
- c) To maintain consistency of supervision, guidance and instruction, Contractor

- agrees that Supervisors will serve for the entirety of the contract term. If a change in Supervisor must occur, it shall be done with the prior agreement of the County.
- d) Contractor is responsible for communicating information to its employees regarding hours of work, duration and location of assignment, expectations, dress code during onsite onboarding and other information concerning the assignment. Prior to assignment with County, Contractor shall ensure that each employee reviews/signs the documents contained in the MCDSS onboarding forms, attached as **Exhibit F** to this Agreement. Contractor shall keep signed onboarding forms for each employee, filed and available upon request.
 - e) Contractor employees provided under the terms of this agreement and shall maintain a professional demeanor.
 - f) Contractor employees shall be provided a copy of County's drug-free policy statement and shall adhere to the policy as a condition of employment under this agreement.
 - g) Contractor employees shall be oriented to the appropriate policy, practice, and procedures determined by the County to be relevant and necessary for Contractor Employees. This orientation will take place during the initial one-week onsite onboarding period.

F. Background Screening

All Contractor employees must complete an initial pre-employment background screening prior to assignment with the County. Contractor is responsible for conducting the screenings, and all screenings will be done at Contractor's expense. Livescan fingerprinting with the Dept. of Justice will be administered to Contractor employees during onsite onboarding if not completed prior.

Contractor shall not assign any Contractor employees with a criminal history report revealing a felony and/or misdemeanor conviction and/or pending case action.

IV. REPORTING REQUIREMENTS

Contractor will provide the County Weekly Productivity Reports. In addition, Contractor will provide the County a Monthly Executive Report that includes a budget update, policy questions, and case productivity summary **Exhibit E**. Monthly productivity will meet or exceed what County expects for Intake and Renewal cases. For Intake cases, Support Specialists are expected to review and update between 8 and 10 cases per worker per day. Renewal case complexity varies significantly; however, each Support Specialist is expected to review and update between 10 and 15 cases per worker per day.

V. PAYMENT PROVISIONS:

COUNTY shall pay **CONTRACTOR** according to the terms set forth in **Exhibit B**, Section I. PAYMENT BY COUNTY. **CONTRACTOR** shall submit a monthly invoice to County's Contract Administrator no later than the tenth (10th) day following the end of the month during which costs were incurred. A summary that includes the type of

EXHIBIT A

Medi-Cal case (i.e., Intake or Renewal) and number of cases worked shall accompany the invoice. The invoice shall be presented in the form set forth in **Exhibit D**. Timesheets and payroll register for each individual reimbursement shall accompany the invoice. Documentation for travel reimbursement shall also accompany the invoice.

The maximum amount to be paid by the **COUNTY** to the **CONTRACTOR** under this Agreement shall not exceed **One-Million Six Hundred Fifty-Four Thousand, Two-Hundred Fifteen dollars (\$1,654,215.00)** per **Exhibit C**, Budget

(remainder of this page internationally left blank)

**MONTEREY COUNTY
DEPARTMENT OF SOCIAL SERVICES**

ADDITIONAL PROVISIONS

I. PAYMENT BY COUNTY:

1.01 Monthly claims/invoices by CONTRACTOR: Not later than the tenth (10th) day of each month, CONTRACTOR shall submit to COUNTY a signed invoice setting forth the amount claimed. All invoices (monthly and final) shall be submitted in the form set forth in **Exhibit D**.

1.02 Final Invoice; forfeiture for late invoice: CONTRACTOR's final month and end of fiscal year invoice is due, and must be received by COUNTY, no later than close of business on **October 10th**. **If the Final Invoice is not received by COUNTY by close of business on October 10th. CONTRACTOR understands and agrees that the reimbursement of CONTRACTOR's final expenses represented by that invoice may be forfeited, and COUNTY shall have no legal obligation regarding it, nor shall COUNTY be required to make any payment towards that untimely/late invoiced claim.**

1.03 Allowable Costs:

a) Allowable costs shall be the CONTRACTOR's actual costs of developing, supervising and delivering the services under this Agreement, as set forth in **Exhibit C**. Only the costs listed in **Exhibit C** as contract expenses may be claimed as allowable costs. Any dispute over whether costs are allowable shall be resolved in accordance with the provisions of 45 Code of Federal Regulations, Part 74, Sub-Part F and 48 Code of Federal Regulations (CFR), Chapter 1, Part 31.

b) Allowable costs for travel expenses incurred while providing services under this Agreement, as set forth in **Exhibit C**, must follow the Monterey County Auditor/Controller's Travel Policy www.co.monterey.ca.us/govenment/departments-a-h/auditor-controller/policies-and-procedures and should be invoiced the current per diem rates for lodging, meals, and mileage up to the rates listed online at www.irs.gov.

1.04 Cost Control: CONTRACTOR shall not exceed by more than twenty (20) percent any contract expense line item amount in the budget without the written approval of COUNTY, given by and through the Contract Administrator or Contract Administrator's designee. CONTRACTOR shall submit an amended budget with its request for such approval. Such approval shall not permit CONTRACTOR to receive more than the maximum total amount payable under this contract. Therefore, an increase in one-line item will require corresponding decreases in other line items.

1.05 Payment in Full:

a) If COUNTY certifies and pays the amount requested by CONTRACTOR, such payment shall be deemed payment in full for the month in question and may not thereafter be reviewed or modified, except to permit COUNTY's recovery of overpayments.

EXHIBIT B

b) If COUNTY certifies and pays a lesser amount than the amount requested, COUNTY shall, immediately upon certification of the lesser amount, notify CONTRACTOR in writing of such certification. If CONTRACTOR does not protest the lesser amount by delivering to COUNTY a written notice of protest within twenty (20) days after CONTRACTOR's receipt of the certification, then payment of the lesser amount shall be deemed payment in full for the month in question and may not thereafter be questioned by CONTRACTOR.

1.06 Disputed payment amount: If COUNTY pays a lesser amount than the amount requested, and if CONTRACTOR submits a written notice of protest to COUNTY within twenty (20) days after CONTRACTOR's receipt of the certification, then the parties shall promptly meet to review the dispute and resolve it on a mutually acceptable basis. No court action may be taken on such dispute until the parties have met and attempted to resolve the dispute in person.

II. PERFORMANCE STANDARDS & COMPLIANCE

2.01 Outcome objectives and performance standards: CONTRACTOR shall for the entire term of this Agreement provide the service outcomes set forth in **Exhibit A**. CONTRACTOR shall meet the contracted level of service and the specified performance standards described in **Exhibit A**, unless prevented from doing so by circumstances beyond CONTRACTOR's control, including but not limited to, natural disasters, fire, theft, and shortages of necessary supplies or materials due to labor disputes.

2.02 County monitoring of services: COUNTY shall monitor services provided under this Agreement in order to evaluate the effectiveness and quality of services provided.

2.03 Notice of defective performance: COUNTY shall notify CONTRACTOR in writing within thirty (30) days after discovering any defects in CONTRACTOR's performance. CONTRACTOR shall promptly take action to correct the problem and to prevent its recurrence. Such corrective action shall be completed and a written report made to the COUNTY concerning such action not later than thirty (30) days after the date of the COUNTY's written notice to CONTRACTOR.

2.04 Termination for cause: Notwithstanding Section 7.02 of the Agreement, if the corrective actions required above are not completed and the report to the COUNTY not made within thirty (30) days, the COUNTY may terminate this Agreement by giving five (5) days' written notice to CONTRACTOR.

2.05 Remedies for Inadequate Service Levels:

- a) For each month that service falls below 80% of the contracted level, CONTRACTOR shall submit to the COUNTY an analysis of the causes of the problem and any necessary actions to be taken to correct the problem. If the problem continues for another month, the COUNTY shall meet with CONTRACTOR to explore the problem and develop an appropriate written corrective action plan with appropriate time frames.

EXHIBIT B

- b) If CONTRACTOR does not carry out the required corrective action within the time frame specified, sanctions shall be applied in accordance with funding source regulations.
- c) Notwithstanding Section 7.02 of the Agreement, if, after the COUNTY notifies CONTRACTOR of any sanctions to be imposed, CONTRACTOR continues in its failure to take corrective action, then COUNTY may terminate this contract by giving CONTRACTOR five (5) days' written notice.
- d) If all appropriate corrective actions are taken but service still falls 80% or more below contracted level, COUNTY and CONTRACTOR may renegotiate the contracted level of service.

2.06 Training for Staff: CONTRACTOR shall insure that sufficient training is provided to its volunteer and paid staff to enable them to perform effectively on the project, and to increase their existing level of skills. Additionally, CONTRACTOR shall ensure that all staff completes Division 21 Civil Rights training.

2.07 Bi-lingual Services: CONTRACTOR shall ensure that qualified staff is available to accommodate non-English speaking, and limited English proficient, individuals.

2.08 Assurance of drug free-workplace: CONTRACTOR shall submit to the COUNTY evidence of compliance with the California Drug-Free Workplace Act of 1990, Government Code sections 8350 et seq., by doing the following:

- Publishing a statement notifying employees that the 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 that will be taken against employees for violations of the prohibition;
- Establishing a drug-free awareness program to inform employees about all of the following:
 - 1) the dangers of drug abuse in the workplace;
 - 2) the organization's policy of maintaining a drug-free workplace;
 - 3) any available drug counseling, rehabilitation, and employee assistance programs;
 - 4) the penalties that may be imposed upon employees for drug abuse violations;
 - 5) requiring that each employee engaged in the performance of the contract or grant be given a copy of the company's drug-free policy statement and that, as a condition of employment on the contract or grant, the employee agrees to abide by the terms of the statement.

III. CONFIDENTIALITY

CONTRACTOR and its officers, employees, agents, and subcontractors shall comply with Welfare and Institutions (W & I) Code Sec. 10850, 45 CFR Sec. 205.50, and all other applicable provisions of law which provide for the confidentiality of records and prohibit their being opened for examination for any purpose not directly connected with the administration of public social services. Whether or not covered by W&I Code Sec. 10850 or by 45 CFR Sec. 205.50, confidential medical or personnel records and the identities of

clients and complainants shall not be disclosed unless there is proper consent to such disclosure or a court order requiring disclosure. Confidential information gained by CONTRACTOR from access to any such records, and from contact with its clients and complainants, shall be used by CONTRACTOR only in connection with its conduct of the program under this Agreement. The COUNTY, through the Director of the Department of Social Services, and his/her representatives, shall have access to such confidential information and records to the extent allowed by law, and such information and records in the hands of the COUNTY shall remain confidential and may be disclosed only as permitted by law.

IV. NON-DISCRIMINATION

CONTRACTOR certifies that to the best of its ability and knowledge it will comply with the nondiscrimination program requirements set forth in this Section.

4.01 Discrimination Defined: The term “discrimination” as used in this contract, is the same term that is used in Monterey County Code, Chapter 2.80 “Procedures for Investigation and Resolution of Discrimination Complaints”; it means the illegal denial of equal employment opportunity, harassment (including sexual harassment and violent harassment), disparate treatment, favoritism, subjection to unfair or unequal working conditions, and/or other discriminatory practice by any Monterey County official, employee or agent, due to an individual’s race, color, ethnic group, national origin, ancestry, religious creed, sex, sexual orientation, age, veteran’s status, cancer-related medical condition, physical handicap (including AIDS) or disability. The term also includes any act of retaliation.

4.02 Application of Monterey COUNTY Code Chapter 2.80: The provisions of Monterey COUNTY Code Chapter 2.80 apply to activities conducted pursuant to this Agreement. Complaints of discrimination made by CONTRACTOR against the COUNTY, or by recipients of services against CONTRACTOR, may be pursued using the procedures established by Chapter 2.80. CONTRACTOR shall establish and follow its own written procedures for the prompt and fair resolution of discrimination complaints made against CONTRACTOR by its own employees and agents, and shall provide a copy of such procedures to COUNTY on demand by COUNTY.

4.03 Compliance with laws: During the performance of this Agreement, CONTRACTOR shall comply with all applicable federal, state and local laws and regulations which prohibit discrimination, including but not limited to the following:

- **California Fair Employment and Housing Act**, California Government Code Sec. 12900 et seq., see especially Section 12940 (c), (h), (1), (i), and (j); and the administrative regulations issued thereunder, 2 Calif. Code of Regulations Secs. 7285.0 et seq. (Division 4 - Fair Employment and Housing Commission);
- **California Government Code Secs. 11135 - 11139.5**, as amended (Title 2, Div. 3, Part 1, Chap. 1, Art. 9.5) and any applicable administrative rules and

EXHIBIT B

regulations issued under these sections; including **Title 22 California Code of Regulations 98000-98413**.

- **Federal Civil Rights Acts of 1964 and 1991** (see especially Title VI, 42 USC Secs. 2000d et seq.), as amended, and all administrative rules and regulations issued thereunder (see especially 45 CFR Part 80);
- **The Rehabilitation Act of 1973**, Secs. 503 and 504 (29 USC Sec. 793 and 794), as amended; all requirements imposed by the applicable HHS regulations (45 CFR Parts 80, 84 and 91); and all guidelines and interpretations issued pursuant thereto;
- **7 Code of Federal Regulations (CFR)**, Part 15 and **28 CFR** Part 42;
- **Title II of the Americans with Disabilities Act of 1990** (P.L. 101-336), 42 U.S.C. Secs. 12101 et seq. and 47 U.S.C. Secs. 225 and 611, and any federal regulations issued pursuant thereto (see 24 CFR Chapter 1; 28 CFR Parts 35 and 36; 29 CFR Parts 1602, 1627, and 1630; and 36 CFR Part 1191);
- **Unruh Civil Rights Act**, Calif. Civil Code Sec. 51 et seq., as amended;
- **Monterey COUNTY Code**, Chap. 2.80.;
- **Age Discrimination in Employment Act 1975**, as amended (**ADEA**), 29 U.S.C. Secs 621 et seq.;
- **Equal Pay Act of 1963**, 29 U.S.C. Sec. 206(d);
- **California Equal Pay Act**, Labor Code Sec.1197.5.
- **California Government Code** Section 4450;
- **The Dymally-Alatorre Bilingual Services Act; Calif. Government Code Sec. 7290 et seq.**
- **The Food Stamp Act of 1977**, as amended and in particular **Section 272.6**.
- **California Code of Regulations, Title 24, Section 3105A(e)**
- **Removal of Barriers to Inter-Ethnic Adoption Act of 1996, Section 1808**

4.04 Written assurances: Upon request by COUNTY, CONTRACTOR will give any written assurances of compliance with the Civil Rights Acts of 1964 and 1991, the Rehabilitation Act of 1973 and/or the Americans with Disabilities Act of 1990, as may be required by the federal government in connection with this Agreement, pursuant to 45 CFR

EXHIBIT B

Sec. 80.4 or 45 CFR Sec. 84.5, and 91; 7 CFR Part 15; and 28 CFR Part 35, or other applicable State or federal regulation.

4.05 Written non-discrimination policy: Contractor shall maintain a written statement of its non-discrimination policies which shall be consistent with the terms of this Agreement. Such statement shall be available to employees, recipients of services, and members of the public, upon request.

4.06 Grievance Information: CONTRACTOR shall advise applicants who are denied CONTRACTOR's services, and recipients who do receive services, of their right to present grievances, and of their right to a State hearing concerning services received under this Agreement.

4.07 Notice to Labor Unions: CONTRACTOR shall give written notice of its obligations under paragraphs 4.01 - 4.08 to labor organizations with which it has a collective bargaining or other agreement.

4.08 Access to records by government agencies: CONTRACTOR shall permit access by COUNTY and by representatives of the State Department of Fair Employment and Housing, and any state agency providing funds for this Agreement, upon reasonable notice at any time during normal business hours, but in no case less than 24 hours' notice, to such of its books, records, accounts, facilities, and other sources of information as the inspecting party may deem appropriate to ascertain compliance with these non-discrimination provisions.

4.09 Binding on Subcontractors: The provisions of paragraphs 4.01 - 4.08 shall also apply to all of CONTRACTOR's subcontractors. CONTRACTOR shall include the non-discrimination and compliance provisions of these paragraphs in all subcontracts to perform work or provide services under this Agreement.

V. ADDITIONAL REQUIREMENTS

5.01 Covenant Against Contingent Fees: CONTRACTOR warrants that no person or selling agency has been employed or retained to solicit this Agreement. There has been no agreement to make commission payments in order to obtain this Agreement. For breach or violation of this warranty, COUNTY shall have the right to terminate this Agreement without liability or, at its discretion, to deduct from the Agreement price or consideration, or otherwise recover, the full amount of such commission, percentage, brokerage, or contingency fee.

5.02 Debarment, Suspension and Fraud, and Abuse: CONTRACTOR certifies to the best of its knowledge and belief, that it and any subcontractors:

- a) Are not presently debarred, suspended, proposed for disbarment, declared ineligible, or voluntarily excluded from covered transactions by any federal or State department or agency.
- b) Have not, within a three-year period preceding this Agreement, been convicted of, or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain,

EXHIBIT B

- or performing a public (federal, State, or local) transaction or contract under a public transaction; violation of federal or State antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property.
- c) Are not presently indicted for, or otherwise criminally or civilly charged by a governmental entity (federal, State, or local) with commission of any of the offenses in 5.02(b).
 - d) Have not, within a three-year period preceding this Agreement, had one or more public transactions (federal, State, or local) terminated for cause or default.

CONTRACTOR shall report immediately to COUNTY in writing, any incidents of alleged fraud and/or abuse by either CONTRACTOR or its subcontractors.

CONTRACTOR shall maintain any records, documents, or other evidence of fraud and abuse until otherwise notified by COUNTY.

CONTRACTOR agrees to timely execute any and all amendments to this Agreement or other required documentation relating to the debarment/suspension status of any subcontractors.

VI. CONTRACT ADMINISTRATORS

6.01 Contract Administrator – CONTRACTOR: CONTRACTOR hereby designates **Renee Carter** as its Contract Administrator for this Agreement. All matters concerning this Agreement which are within the responsibility of CONTRACTOR shall be under the direction of, or shall be submitted to, the CONTRACTOR's Contract Administrator. CONTRACTOR may, in its sole discretion, change its designation of the Contract Administrator, and shall promptly give written notice to COUNTY of any such change.

6.02 Contract Administrator – COUNTY: COUNTY hereby designates the Director of the Monterey County Department of Social Services as its Contract Administrator for this Agreement. All matters concerning this Agreement which are within the responsibility of COUNTY shall be under the direction of, or shall be submitted to, the Director or such other COUNTY employee in the Department of Social Services as the Director may appoint. COUNTY may, in its sole discretion, change its designation of the Contract Administrator, and shall promptly give written notice to CONTRACTOR of any such change.

VII. CONTRACT DEPENDENT ON GOVERNMENT FUNDING

COUNTY's payments to CONTRACTOR under this Agreement are funded by the State and Federal governments. If funds from State and Federal sources are not obtained and continued at a level sufficient to allow for COUNTY's purchase of the indicated quantity of services, then COUNTY may give written notice of this fact to CONTRACTOR, and the obligations of the parties under this Agreement shall terminate immediately, or on such date thereafter, as COUNTY may specify in its notice, unless in the meanwhile the parties enter into a written Amendment modifying this Agreement.

VIII. APPEAL PROCESS

In the event of a dispute or grievance regarding the terms and conditions of this Agreement, both parties shall abide by the following procedures:

- a) CONTRACTOR shall first discuss the problem informally with the designated DSS Contact/Program Analyst. If the problem is not resolved, CONTRACTOR must, within fifteen (15) working days of the failed attempt to resolve the dispute with DSS Contact/Program Analyst, submit a written complaint, together with any evidence, to the DSS Branch Deputy Director. The complaint must include a description of the disputed issues, the legal authority/basis for each issue which supports CONTRACTOR's position, and the remedy sought. The Branch Deputy Director shall, within fifteen (15) working days after receipt of CONTRACTOR's written complaint, make a determination on the dispute, and issue a written decision and reasons therefore. All written communication shall be pursuant to Section 14. NOTICES of this Agreement. Should CONTRACTOR disagree with the decision of the Division Deputy Director, CONTRACTOR may appeal the decision to the Director of the Department of Social Services.
- b) CONTRACTOR's appeal of the Branch Deputy Director's decision must be submitted to the Department Director within ten (10) working days from the date of the decision; be in writing, state the reasons why the decision is unacceptable, and include the original complaint, the decision that is the subject of appeal, and all supporting documents. Within twenty (20) working days from the date of CONTRACTOR'S appeal, the Department Director, or his/her designee, shall meet with CONTRACTOR to review the issues raised on appeal. The Department Director shall issue a final written decision within fifteen (15) working days of such meeting.
- c) CONTRACTOR may appeal the final decision of the Department Director in accordance with the procedures set forth in Division 25.1 (commencing with Section 38050) of the Health and Safety Code and the regulations adopted thereunder. (Title 1, Subchapter 2.5 commencing with Section 251, or Subchapter 3 commencing with Section 300, whichever is applicable, of the California Code of Regulations).
- d) CONTRACTOR shall continue to carry out the obligations under this Agreement during any dispute.
- e) Costs incurred by CONTRACTOR for administrative/court review are not reimbursable by COUNTY.

**SolutionsWest
Budget
October 1, 2023 – September 30, 2024**

BUDGET CATEGORIES	BUDGET TOTALS
Personnel	
Project Manager/\$81.00 per hour/1 FTE	\$157,464
Supervisor/\$67.00 per hour/2 FTE	\$260,496
Support Specialist/\$62.50 per hour/10 FTE	\$1,215,000
Total Salaries	\$1,632,960
Total Personnel	\$1,632,960
Onboarding Week Expenses*	
Lodging for On Site Onboarding week \$166.00/night for 5 nights	\$14,625
Travel	\$2,730
Per Diem for On Site Onboarding week \$60.00/day for 5 days	\$3,900
Total Onboarding	\$21,255
TOTAL	\$1,654,215

*Onboarding Reimbursement: County and CONTRACTOR agree that CONTRACTOR shall be reimbursed for travel expenses during this Agreement. One Time Travel Costs are calculated for each resource based on an average hotel expense of \$166/per night for five (5) nights, weekly total transportation of \$210, and a \$60 per diem for meals & incidentals. To receive reimbursement, CONTRACTOR must provide a detailed breakdown of authorized expenses, identifying what was expended and when. (As per County/IRS reimbursement guidelines <https://www.gsa.gov/travel/plan-book/per-diem-rates>)

The maximum amount to be paid by COUNTY to CONTRACTOR under this Agreement shall not exceed **One-Million Six Hundred-Four Thousand, Two-Hundred Fifteen dollars (\$1,654,215)**



P.O. Box 162639 | Sacramento, CA 95816-2639
 916.469.9949 | www.solutionswest.com

Attn: Aaron McDouglas, Management Analyst II
 Monterey County Department of Social Services
 713 La Guardia, Suite A
 Salinas, CA 93905

Invoice #:
Invoice Date

Contract ID Solutions West, Inc
Amount of this Invoice:

Monterey County DSS Medi-Cal Support Services,

Personnel						Total Hours	Rate	Total
Project Manager						0.0	\$ 81.00	\$ -
Project Supervisor						0.0	\$ 67.00	\$ -
Project Supervisor						0.0	\$ 67.00	\$ -
Support Specialist 1						0.0	\$ 62.50	\$ -
Support Specialist 2						0.0	\$ 62.50	\$ -
Support Specialist 3						0.0	\$ 62.50	\$ -
Support Specialist 4						0.0	\$ 62.50	\$ -
Support Specialist 5						0.0	\$ 62.50	\$ -
Support Specialist 6						0.0	\$ 62.50	\$ -
Support Specialist 7						0.0	\$ 62.50	\$ -
Support Specialist 8						0.0	\$ 62.50	\$ -
Support Specialist 9						0.0	\$ 62.50	\$ -
Support Specialist 10						0.0	\$ 62.50	\$ -
Total Hours	0	0	0	0	0	0.00		

**** Weekly approved time reports attached.**

Total **\$ -**

Invoice Contact Information

Submitted by: Renee Carter, SolutionsWest, (916) 765-7886

Remit to
 Solutions West Inc
 Box 162639
 Sacramento, CA 95816

I certify that this invoice is true and correct to the best of my knowledge.



CONFIDENTIALITY POLICY ACKNOWLEDGEMENT

I, _____, hereby certify that I have received information pertaining to my responsibilities, the policies, procedures and laws regarding maintaining the confidentiality of client records and information with the department. I understand that confidentiality is mandated by the State of California, Welfare and Institutions Code Section 10850, Section 19 of the State Operations Manual, Civil Code Section 1798, and the department administrative directives regarding confidentiality and handling sensitive cases. I have been informed that any willful or knowing violation of the law is a misdemeanor and that breach of confidentiality is grounds for disciplinary action up to and including dismissal.

Signature

Date



Acknowledgement of Understanding and Receipt of Administrative Directive 11-03 Handling of Sensitive Cases

I [redacted] have been provided with a copy of the Monterey County Department of Social Services' Handling of Sensitive Cases Administrative Directive 11-03.

I understand I cannot access my own case record(s), cases of relatives, people known to me or case(s) for which I am an Authorized Representative.

My acknowledgment of my understanding of the policies within and my receipt of this Administrative Directive are indicated by my signature below.

Employee Signature

[redacted]

Date



Administrative Directive No. 23-05

TO: All DSS Staff
DATE: August 1, 2023
SUBJECT: Policies for Sensitive Cases
OBSOLETES: Administrative Directive 11-03

SUMMARY

This Administrative Directive provides policies for cases administered in the County of Monterey Department of Social Services (DSS) program branches that are deemed sensitive due to their high-profile nature, potential for conflict of interest or safety need.

DEFINITIONS

- **Authorized Representative:** A representative is a person who has been chosen to act or make decisions on behalf of another person who receives services from the Department of Social Services.
- **Conflict of Interest:** A “conflict of interest” exists when a public employee's private interests could improperly influence or appear to influence performance of their official duties, responsibilities and/or decision-making.
- **Case:** A case, in this document refers to services and or programs administered by the Department of Social Services.
- **Other relationships:** Includes persons related to a current or former employee who is a household member, current or ex significant other, boyfriend, girlfriend, their new partner, former spouse(s), i.e. ex-husband, ex-wife, ex in-laws, or other parent of the employee's or ex's child(ren).
- **Related persons:** Includes person related to a current or former employee and includes but is not limited to: a spouse, husband, wife, civil or domestic partner, child, step-child, foster child, parent, grandparent, sibling, aunt, uncle, niece, nephew, cousin, mother-in-law, father-in-law, daughter-in-law, son-in-law, sister-in-law, brother in-law, etc.

SENSITIVE CASE POLICIES

1. A sensitive case status will be assigned for applicants and recipients of public welfare services or benefits when the case involves a current or former employee, their relative/other relation and/or the employee serves as an authorized representative.
2. Cases involving employees from other departments, elected official`s or any other individual determined to need or request special handling may be assigned a sensitive case status.
3. Procedures for labeling a case as sensitive are located on the Branch SharePoint page.

The following criteria assists staff in identifying individuals that meet the sensitive case criteria.

- Current employee as an applicant, recipient, caretaker relative, absent parent, or Authorized Representative (AR).
- Customers working in the office where the case is located, i.e., GA Work Program, Summer Youth Program, Court Division Program, or CWES Placement.
- Related persons and other relationships as defined on page one.
- County employees from other departments, elected officials, or any other individual determined to need or requesting special handling.

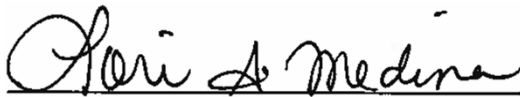
POLICIES FOR EMPLOYEES OR EMPLOYEE AUTHORIZED REPRESENTATIVES APPLYING FOR OR RECEIVING PUBLIC WELFARE SERVICES OR BENEFITS

1. Follow all confidentiality protocols as required by law and referenced in AD 23-04 Confidentiality of Customer/Client Information including but not limited to:
 - a. The use of computers and access to confidential files and images are available only to employees of DSS who have a job related need to know.
 - b. Employees shall not view or access their own case(s) or any case if it in any way personally involves the employee.
 - i. Understand that the CalSAWS and CWS/CMS systems have enhanced tracking ability to determine when cases are accessed by employees. County ITD, DSS ITD, supervisors and managers have access to audit trails within the CalSAWS and CWS/CMS systems to ensure that confidentiality policies are followed.
2. Complete the Conflict of Interest training and Disclosure Form at onboarding and as assigned each year.
3. Report all real or potential conflict of interests to your supervisor, HR or your manager when they arise.
4. Handle all personal case or authorized representative business during your personal time.

- a. Accessing your own case records or those of relatives, friends, household or other relations is prohibited.
- b. Personal use of the county computers, equipment, and supplies to communicate via phone, voicemail, or U.S. mail is prohibited.
- c. Mail correspondence between DSS staff related to the employee's case is handled through normal channels (U.S. Mail). Therefore, correspondence may not be e hand-delivered or left on an employee's desk.
- d. The County Network is strictly for official use only.

BRANCH RESPONSIBILITIES

1. All Branches: Ensure all case carrying staff have access to the procedures for initiating and managing a sensitive case.
2. HR Branch: Assign the Conflict of Interest training and Disclosure Form to all employees at onboarding and annually.
 - a. Inform the Branch Senior Secretary and Deputy Director when any conflicts are identified.



Lori A. Medina
DSS Director



Acknowledgement of Understanding and Receipt of Administrative Directive 23-03 Conflicts of Interest

I [redacted] have been provided with a copy of the Monterey County Department of Social Services' Conflicts of Interest Administrative Directive 23-03.

I understand I am required to disclose any and all real or perceived conflicts of interest as soon as I become aware of them and annually as assigned by DSS Human Resources.

My acknowledgment of my understanding of the policies within and my receipt of this Administrative Directive are indicated by my signature below.

Employee Signature

[redacted]

Date



W O R K I N G T O G E T H E R F O R O U R C O M M U N I T Y

Administrative Directive No. 23-03

TO: All Staff

DATE: February 20, 2023

SUBJECT: Conflicts of Interest

REFERENCES: [Handling of Sensitive Cases](#)
[Declaration of Outside Employment](#)
[Monterey County Policy on Family and Romantic Relationships at Work](#)

OBSOLETE: Obsoletes Administrative Directive 19-08

DEFINITIONS: **Conflict of Interest:** A “conflict of interest” when a public employee's private interests could improperly influence or appear to influence performance of their official duties, responsibilities and/or decision-making.

Case: Services and or programs administered by the Department of Social Services.

Related persons: Includes but is not limited to: a spouse, husband, wife, civil or domestic partner, child, step-child, foster child, parent, grandparent, sibling, aunt, uncle, niece, nephew, cousin, mother-in-law, father-in-law, daughter-in-law, son-in-law, sister-in-law, brother-in-law, etc.

Other relationships: household members, current or ex significant others i.e. boyfriends, girlfriends, their new partners, former spouse(s), i.e. ex-husband, wife, ex in-laws, other parent of the employee's or ex's child(ren).

Authorized Representative: A representative is a person who has been chosen to act or make decisions on behalf of another person who receives services from the Department of Social Services.

I. PURPOSE

The potential which exists for conflicts between an employee’s job duties and the employee’s private interests is something about which all staff must be concerned.

Conflicts of interest, in addition to being prohibited by law, can be detrimental to our clientele, staff, and the Department of Social Services (DSS).

Demonstration of the highest standards of personal integrity, truthfulness, honesty and fortitude in all our professional activities is required in order to inspire public confidence and trust. In this regard, the public often has a higher expectation of us, as public servants, which may require us to assess even the appearance of a conflict of interest in our actions. This directive confirms and restates the Department's conflict of interest policies and procedures.

II. POLICIES AND PROCEDURES

1. All situations of potential conflicts of interest shall be immediately brought to the attention of a supervisor and DSS Human Resources.
 - a. Supervisors, in turn, must notify the Program Manager.
2. In addition, all employees shall annually complete the [Declaration of Conflict-of-Interest Form](#) as assigned by DSS Human Resources.
3. DSS Human Resources and Branch management will then work to appropriately and effectively address and resolve all real and perceived conflicts of interest.
4. Employees are prohibited from accessing any departmental case or client information for which they have no business need or with whom they have a relationship to or are related or with whom they are serving as an authorized representative (see definitions above).
5. An employee shall not be assigned to any case and shall not perform any action on any case if it in any way personally involves the employee. This includes but is not limited to CalWORKs benefits issuance (i.e., EBT, CalFresh, Medi-Cal, MC- Choice, General Assistance), employment services and social work services cases which involve the employee's relatives, family members, household members, personal friends, ex's, ex's new interest, etc. and individuals with whom there is a business relationship etc. as defined above.

This includes casework, clerical, and any other official departmental activities.

- a. Program and Branch Managers shall arrange for the work on such cases to be done by a limited number of uninvolved staff.
 - b. Program and Branch Managers will also arrange to receive a monthly report on the assignment of the cases to ensure an even distribution of sensitive cases to assigned staff.
6. Employees are prohibited from directly supervising related persons and may not make, participate in making, or influence any employment decision involving a related person or one with whom they have a relationship.
7. Employees shall not charge, request, or receive any fee, reward, gift, or payment of any kind from any person in exchange for providing County and Departmental services to any person. This prohibition does not apply to fee collection activities authorized as part of the operation of a program.

8. Employees shall not provide services or goods to clients of the Department other than those which are appropriately provided under the rules of the various programs administered by the Department. Such conflicts of interest would include, but are not limited to:
 - a. Establishing legal relationships such as power of attorney, durable power of attorney, guardianship of conservatorship with clients.
 - b. Referring clients to professionals who are personal friends or accepting departmental clients in a private client role where one expects to receive personal remuneration for providing services.
 - c. Engaging in business relationships with clients
 - d. Benefiting personally in some financial manner from clients
 - e. Being a beneficiary of a client's estate or insurance policy
9. Employees shall not solicit among County employees on County property or during work time for the purpose of providing professional or other services to them. This prohibition does not apply to legitimate employee bargaining unit activities.
10. No employee shall participate in making any departmental decision regarding any agency, board, or organization in which the employee holds an official position.
11. No employee shall receive gifts from potential vendors when in a decision-making position regarding contracts or purchases.
12. No employee shall participate in a decision involving a contract, vendor or services if the employee's family member or significant other is involved.

III. RESPONSIBILITY

It is the responsibility of all staff to be aware of and comply with these policies. Any questions regarding the interpretation of these policies shall be promptly discussed by the employee with their supervisor. The supervisor will consult with the Department of Social Services Human Resources Branch, for further clarification regarding interpretations of these policies.

It is the responsibility of the individual employee, Department managers and supervisors to ensure that each employee understands and complies with these policies. Non-compliance with these policies shall result in corrective action, which may include discipline up to and including termination.

DocuSigned by:

DF027950448749D...
Lori A. Medina
Director



**Acknowledgement of Understanding and Receipt of
Administrative Directive 00-03
Department Computer Policy Statement and Agreement**

I have been provided with a copy of the Monterey County Department of Social Services' Department Computer Policy Statement and Agreement Administrative Directive 00-03.

My acknowledgment of my understanding of the policies within and my receipt of this Administrative Directive are indicated by my signature below.

Name

Employee Signature

Date



Administrative Directive No. 00-03

TO: All Staff January 31, 2000

SUBJECT: Department Computer Policy Statement and Agreement

IMPLEMENTATION: Upon Receipt

I. PURPOSE

This Administrative Directive provides policy and procedures for users of county, state and federally provided computer equipment. This includes, but is not limited to, individual desktop and laptop workstations, printers and network equipment. It is the responsibility of every user to safeguard the equipment provided to them.

This directive provides important policy and procedures, which will:

- Minimize the potential for damage to workstations and equipment,
- Assure legal compliance with software usage,
- Assure maintenance of original configurations for easier troubleshooting, and
- Assure compliance with state system mandates.

II. POLICIES

A. It is expected that Users of all computer equipment **will not**:

1. Install any personal software, including screen savers, without written authorization from Administrative Services Division (ASD). Only standard screen savers and wallpapers that came with the system may be used. This is to protect against the introduction of viruses to the networks and comply with contractual maintenance agreements.
2. Make any modification or configuration changes to network workstations (CMS, ISAWS) without the prior written approval of the Information Technology Manager for that system. This includes saving of any unauthorized, executable (.exe) files to the hard drive.
3. Make unauthorized copies of county-owned software for personal, home or other use.
4. Use "shareware" or other legally free software unless authorized by the PC Support Analyst in ASD.
5. Copy in any form licensed, commercial software programs and/or written user materials such as manuals for personal computers.

6. Use any software or hardware for violating copyright, licensing agreements, trade secrets, personal use, entertainment, counterfeiting, fraud, breach of confidentiality or any other unlawful and or unauthorized purpose.
7. Create a breach of security such as: "hack" into unauthorized areas, share confidential passwords, cause information integrity to be in question, create and/ or activate a computer virus or any other destructive operation or connect to unauthorized networks.
8. Monitor any electronic functions for the purpose of fraud, breach of confidentiality, invading personal privacy, personal use, exploitation in any form, or any other unlawful and/or unauthorized purpose (i.e., E-mail messages or Network access).
9. Install and/or use software for personal use including but not limited to: letters, correspondence labels, databases of any kind, games, gambling, keeping track of pools, raffles, programs to figure odds, stock market tracking, and real estate transactions.
10. Take floppy disks home to complete work, unless a virus protection program is installed on the home computer and the disk is scanned for virus prior to using it on any DSS computer.
11. Inquire into cases/referrals not in their own caseload or those of their unit or buddy unit. This includes any inquiries into information that is not related to the performance of an employee's authorized job duties. The Department may provide confidential services to its own employee's and their relatives. Such cases/referrals are designated as "Sensitive" and the Department is committed to maintaining strict confidentiality. The policies outlined in the current "Confidentiality of Information" Administrative Directive, applies to all cases/referrals and staff.
12. Write anonymous entries into case comments or send anonymous messages over a network mail system. The Department expects that all communication be conducted in a professional manner and that the author takes responsibility for their case entries or comments.
13. Share passwords or user id's for access into any system. Passwords are a unique means to protect Department equipment and data. Passwords should be changed on a regular basis and not be shared with others unless the nature of the work environment calls for common passwords.

B. In addition, it is expected that ISAWS computer users **will not**:

1. Make changes to default settings on any shared workstations.
2. Change Microsoft NT standardized settings such as color, wallpaper, screen savers, and so on. **This includes the creation of custom colors and wallpapers.** Changes in settings may affect the ISAWS application requiring reprogramming by authorized staff.
3. Enter directory areas or open system files for any reason.
4. Enter the Control Panel except to activate Microsoft NT standardized wallpapers and screen savers.

C. Equipment Maintenance

1. It is expected that Users of all computer equipment **will not**:
 - a) Eat or drink at or near the computer workstations or equipment. Food or beverage damage can make the workstation inoperable necessitating costly repair and/or replacement.
 - b) Place magnets or items with magnets on the CPU or monitor. Magnets cause malfunction of the hard drive and diskettes.
 - c) Drop paper clips or staples into the keyboard. These can cause damage.
 - d) Write on or highlight any of the keys on the keyboard or any other part of the computer workstation or equipment.
 - e) Plug any electronic devices with a heating element, such as mug warmers, space heaters, coffee pots, hot pots or halogen lamps in the same electrical outlet as the computer. These items use large amounts of power and may cause circuit overloads and damage to the computer.
 - f) Relocate any CMS or ISAWS workstation, mouse or keyboard. This is to be done by CMS or ISAWS Information Technology Staff. Advanced notification of at least 48 hours is requested.
 - g) Relocate a mouse or keyboard from an unoccupied workstation to replace equipment removed for repair or replacement. This is to be done, only when necessary, by CMS or ISAWS Information Technology Staff.
 - h) Use more than 3-4 monitor blocks under the monitor, as this is a safety risk and the monitor can easily be tipped over.

- i) Install any private printers to the ISAWS Computers. Requests for private printers will be reviewed by the Administrative Services Division and installed by ISAWS Information Technology upon approval.
 - j) Take equipment home for personal use, including but not limited to, mouse, wrist rests, glare screens, etc.
 - k) Damage or misuse any equipment based on the policies within this directive. Damage or misuse shall result in corrective action, which may include disciplinary action up to and including termination.
2. It is expected that all Users of computer equipment **will**:
- a. Sign in and out all portable equipment, such as laptop computers, with the appropriate Information Technology Staff.
 - b. Sign in and out all portable equipment such as emulators, overhead projectors, PA systems, TVs and VCRs from Human Resources.
 - c. Return all portable equipment in the same condition that it was in when it was signed out. It is expected that Portable equipment will not be left on an unattended desk, as it may need to be locked up.
 - d. Report all non-functioning equipment, including portable equipment, immediately upon return to the appropriate Information Technology Staff so that necessary repairs can be made.

D. Acceptable Uses of Networks:

Department of Social Services provided network access is intended to be used to conduct Department business. Employees are encouraged to use technical resources as an efficient and effective business tool.

It is expected that Networks will be used in a manner that does not jeopardize security, confidentiality, or potentially subject the Department to litigation as a result of breaking any local, state or federal law related to privacy, public record or copyright.

E. Unacceptable Uses of Networks:

Department provided network access may not be used for transmitting, retrieving, or storing of any communications of a discriminatory or harassing nature or materials that may be perceived as obscene. Harassment of any kind is prohibited by Department and County policy. No messages with derogatory or inflammatory remarks about race, age, disability, religion, national origin, physical attributes, sexual preference or pornographic nature shall be transmitted. No abusive, profane or offensive language or pictures will be transmitted through the Department's network.

H. Computer Information:

All computer information created utilizing Department computing resources is the property of the Department. It is subject to applicable legal privileges and confidentiality requirements. All computer information entered on Department computers is not private and is subject to disclosure upon the demand of authorized Department offices at any time. The physical location of the computer does not alter this policy. Unauthorized printing or changing of computer information is not allowed. As a condition of initial and/or continuing usage of the Department's e-mail/Internet facilities and resources, all employees are deemed to have consented to Department review and/or disclosure of e-mail/Internet records. E-mail/Internet records are to be treated like shared paper files, with the expectation that anything in them is available for review by authorized Department representatives. Employees have no right or expectation of privacy in e-mail/Internet communications. E-mail/Internet records may be subject to disclosure to law enforcement and/or government officials, or to other third parties through the Public Records Act request, formal discovery process, specific applicable statutes, or other process. Consequently, employees shall ensure that the business information contained in e-mail/Internet records is accurate, appropriate and lawful. The Department reserves the right to disclose employee e-mail/Internet records to law enforcement or government officials, or to other third parties without prior notification to or permission from the employee sending or receiving such records.

I. Implementation:

This Administrative Directive will be reviewed with staff at Benefits Orientation, New Employee Orientation or on the first day of employment, but no later than the fifth day of employment, and the signature sheet will be retrieved and submitted directly to Human Resources for filing in the employee's personnel record.

The policies listed in this Administrative Directive are in accordance with the policies issued by the County Human Resources & Employment Services Division.

Information Technology Staff have the authority to remove any unauthorized files or programs if the user does not remove them upon request.

This policy will be reviewed periodically for appropriateness and applicability, and may be modified within the sole discretion of the Department.

III. RESPONSIBILITY

It is the responsibility of all staff to be aware of and comply with these policies. Any questions regarding the interpretation of these policies shall be promptly discussed by the employee with his or her supervisor. The Supervisor will consult with Administrative Services Division Information Technology staff if any conflicts regarding interpretations arise.

It is the responsibility of all Department Managers and Supervisors to ensure that each employee understands and complies with these policies. Non-compliance with these policies shall result in corrective action, which may include disciplinary action up to and including termination.

/s/ Marie Glavin
Marie Glavin
Director

02/01/00
Date

I have been provided with a copy of the Monterey County Department of Social Services' Computer Policy Statement and Agreement. My acknowledgment of its receipt and my understanding of the policy are indicated by my signature below.

I understand that a copy of this acknowledgement will be placed in my personnel file.

Employee Name (Please Print)

Employee Signature

Date



MCDSS SYSTEM SECURITY AGREEMENT ACKNOWLEDGMENT

I have been provided with a copy of the Monterey County Department of Social Services Systems Security Agreement. My acknowledgment of its receipt and my understanding of this agreement are indicated by my signature below.

Employee Name

Employee Signature

Date

MCDSS Systems Security Agreement

As a Monterey County Department of Social Services (MCDSS) employee, you will be granted access to confidential information that is contained within certain County, State and Federal systems including the C-IV System, California Healthcare Eligibility, Enrollment and Retention System (CalHEERS) and Medi-Cal Eligibility Data System (MEDS). This confidential information includes but is not limited to all County, State (including but not limited to all State Automated Welfare Systems (SAWS) and/or Federal information, data, and information processing resources to which you may have access, and information received from any recipient or applicant for public assistance.

As a MCDSS employee, you are responsible for protecting the Confidential Information of applicants and recipients by following the security procedures set forth below and the policies contained within Administrative Directives 11-01, Confidentiality of Customer-Client Information and 03-01, Conflicts of Interest.

By signing below, you attest to your understanding of the following security responsibilities:

1. All data in any County, State and/or Federal systems accessed in the course of your job duties including the C-IV, CalHEERS and MEDS Systems is confidential and shall not be disclosed to any unauthorized person(s) or group(s).
2. You may use any County, State and/or Federal systems including the C-IV, CalHEERS and MEDS Systems accessed in the course of your duties, **only** for those specific functions for which you are authorized. Personal, non-county, and/or unauthorized use of these systems is prohibited.
3. You may not access, update or perform work on any case in any County, State and/or Federal systems including the C-IV, CalHEERS or MEDS systems accessed in the course of your duties on your own case records, the case records of family members or the case records of anyone that you are acquainted with personally or professionally.
4. In the course of your duties and assigned responsibilities, you may only access these systems and information while at a County operated facility and while using County maintained and controlled equipment and internet access; you may not access these systems or data off-site or through any personal equipment or internet connection without the prior express written permission of the Director of DSS or their designee.
5. For Regional Call Center (RCC) workers and their back-ups, your universal access to the C-IV, CalWIN, and LEADERCounty's data is granted for the sole purpose of carrying out your assigned duties as an RCC agent only during your scheduled work hours.
6. You understand it is illegal for you to knowingly access any of the systems used in the course of your duties as a MCDSS employee, to delete, share, disclose, release, damage, destroy, or copy applicant, recipient, and/or participant information, post any information found in these systems on the Internet, or otherwise use any County, State and/or Federal system including the C-IV, CalHEERS and MEDS Systems, in an unlawful manner including to defraud, deceive, extort, or control data for personal gain.

MCDSS Systems Security Agreement

7. You are not permitted to leave any County, State and/or Federal system including the C-IV, CalHEERS and/or MEDS Systems unattended at any time. When leaving any County, State and/or Federal system including a C-IV Workstation, you must log off or lock that System.
8. Any suspected violation of this *MCDSS Systems Security Agreement*, and any misuse or non-compliance with the C-IV operating standards and procedures, shall be reported immediately to the appropriate County entity.
9. Your violation of this Agreement will result in denied access to any County, State and/or Federal system including the C-IV, CalHEERS and MEDS Systems used in the course of performing your duties and you may be subject to discipline, up to and including termination from employment, and prosecution under the California Penal Code.
10. In addition to and independent of any action taken indicated in paragraph 8, above, abuse of the privileges provided herein, and/or the misuse of any County, State and/or Federal system including the C-IV, CalHEERS and MEDS Systems outside of the scope of employment or assigned duties pursuant to this Agreement may subject the violator to personal civil and/or criminal liability.

I acknowledge that my supervisor has reviewed with me and that I have read and understand the entirety of this Agreement and agree to the terms herein.

Print Employee Name	Employee Signature	Date
Print Supervisor Name	Supervisor Signature	Date



**INFORMATION TECHNOLOGY POLICIES
ACKNOWLEDGMENT FORM**

By my signature, I acknowledge that I have been provided with a copy of the following policies:

- Monterey County 1. Information Technology Security Policy
- Monterey County 2. Information Technology Appropriate Use Policy
- Monterey County 3. Information Technology Data Privacy Policy
- Monterey County 4. Information Technology Social Media Usage Policy

Employee Name

Employee Signature

Date

Monterey County



Subject: Security Policy
Date Issued: May 13, 2014
Issued by: Information Technology Governance Committee
Approved by: The County of Monterey Board of Supervisors
Applies to: All County Officials, Employees and Affiliates

1. INFORMATION TECHNOLOGY SECURITY POLICY

1.1. POLICY PURPOSE

The purpose of this policy is to establish County-wide information security practices which protect and secure County information and information technology resources from intrusion and misuses, as required by California and federal law and as recommended by industry best practices.

1.2. POLICY SCOPE

This policy applies to all County employees and affiliates.

1.3. DEFINITIONS

- 1.3.1. Affiliates – Includes but is not limited to, third party contractors, volunteers, advisory and other committee and commission members, vendors, or others associated with the County in order to accomplish County business.
- 1.3.2. Information Owner - The official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. Generally, this role falls upon a Department Head.
- 1.3.3. Information Technology Resource - All computers, peripherals, and related equipment and software; voice communications infrastructure, peripherals, and related equipment and software; data communications infrastructure, peripherals, and related equipment and software; all other associated tools, instruments, and facilities; and the services that make use of any of these technology resources. The components may be individually controlled (i.e., assigned to an employee) or shared in a single-user or multi-user manner; they may be stand-alone or networked; and they may be stationary or mobile.
- 1.3.4. Information Security Team – A team of individuals who work for and report directly to the Chief Security and Privacy officer and assist in executing the Chief Security and Privacy Officer’s responsibilities as directed.
- 1.3.5. Business Associate Agreement – A written agreement to refrain from using or disclosing department information other than as permitted or required by the Agreement or as

required by law and to use current industry safeguards to prevent use or disclosure of department information covered by the agreement or as required by law.

- 1.3.6. Computer – Any computing resource that accesses, stores or otherwise provides connectivity to County information, including but not limited to devices such as desktop computers, servers, smart phones, tablets and laptops.

1.4. **ROLES AND RESPONSIBILITIES**

The County has established the following Information Security roles and responsibilities:

- 1.4.1. **Chief Security and Privacy Officer (Chief Security and Privacy Officer).** To achieve the goals of this Policy, a Chief Security and Privacy Officer position shall be maintained within the County. The County Board of Supervisors authorizes the County's Chief Security and Privacy Officer to develop and maintain the County's Information Security Program and requires all County Departments to comply. Specific guidance, direction, and authority for information system security are centralized for the County and its subsidiaries in the role of the Chief Security and Privacy Officer. The Chief Security and Privacy Officer shall:
 - 1.4.1.1. Implement, administer, and interpret County Information Security Policies
 - 1.4.1.2. Establish and maintain Information Security Standards in support of Information Security Policy, laws and regulations. Standards consist of specific low level mandatory controls that help enforce and support the information security policy
 - 1.4.1.3. Establish, provide and maintain Information Security guidelines and best practices. Guidelines consist of recommended, non-mandatory controls that help support standards or serve as a reference when no applicable standard is in place
 - 1.4.1.4. Oversee the assessment of Information Security risks and oversee policy, legal and regulatory gap analyses with the assistance, as requested, of County Counsel
 - 1.4.1.5. Recommend technologies, practices and appropriate corrective actions to mitigate Information Security risks
 - 1.4.1.6. Review and assess the risk of technical changes that affect County security posture
 - 1.4.1.7. Promote County-wide information security awareness
 - 1.4.1.8. Interpret laws and regulations as they apply to County information security practices
 - 1.4.1.9. Adopt best practices and recommendations from agencies such as NIST, CERT, SANS, DOD, and implement as necessary to preserve information technology resources and information
 - 1.4.1.10. Oversee the security and intrusion monitoring of the County's networks
 - 1.4.1.11. Oversee a Security Incident Response Team as a multi-disciplinary organized team that is trained to respond to major security incidents
 - 1.4.1.12. Oversee information technology-related forensic investigations as directed by County Counsel, the District Attorney's Office, or a law enforcement agency
 - 1.4.1.13. Audit compliance with County Information Security Policy and Standards and provide vulnerability assessment and reporting for the purposes of:

Fulfilling the County Board of Supervisors' Response to the Monterey County Civil Grand Jury 2004 Final Report, which stipulates that the Chief Security and Privacy Officer have access to all systems for the purpose of auditing compliance with the

Board's adopted policies, security incident investigation and response, and counsel-directed investigation activities,

- 1.4.1.13.1. The Chief Security and Privacy Officer shall have comprehensive around-the-clock system administrator/superuser rights to all network-connected County devices except for standalone un-networked County devices, or those County devices attached only to an isolated LAN.
 - 1.4.1.13.1.1. For the purpose of this Policy, an isolated LAN is defined as a network for which all connectivity is contained to a single building and limited to use by a single department, affording the network and its connected devices protection by physical security measures. Physical access to these standalone un-networked computers and isolated LANs shall be provided to the Chief Security and Privacy Officer on request.
 - 1.4.1.13.1.2. Unless written direction has been issued by County Counsel, the District Attorney's Office, or a law enforcement agency, physical access to computers shall be coordinated with the appropriate department information owner(s) (defined in section 1.4.2). Physical access may be restricted where limited by law, regulation or written departmental policy.
 - 1.4.1.13.1.3. No department information shall be intentionally accessed without the written direction of the County Counsel's office, the District Attorney's Office, a law enforcement agency, or the affected department(s).
 - 1.4.1.13.1.4. The access granted to the Chief Security and Privacy Officer shall not be utilized to grant similar access to anyone outside of the Chief Security and Privacy Officer's Information Security team.
 - 1.4.1.13.1.5. The Information Technology department shall enter into Business Associate Agreements with departments whose information is protected by law so that in the event of any incidental contact with that protected information, the Information Technology department shall be accountable to maintain the confidentiality and privacy required to meet applicable laws and regulations.
 - 1.4.1.14. Maintain a separation-of-duties security program. While the Chief Security and Privacy Officer shall partner with County departments toward their success and the fulfillment of their business goals, the Chief Security and Privacy Officer shall not control the IT business nor possess the authority or responsibility for the support and maintenance of the day-to-day production IT environment. By maintaining a "separation of duties" security program, the Chief Security and Privacy Officer shall be able to both advise the County and audit its security as well. The Chief Security and Privacy Officer shall be responsible, however, for overseeing the compliance of the IT department with County Policies, Standards and best practices.
 - 1.4.1.15. Have appropriate staff and effect appropriate security management under the authority of the Director of Information Technology and the County Administrative Officer.
 - 1.4.1.16. Collaborate with and coordinate departmental information protection actions with the County's departmental Information Security Officers.
- 1.4.2. **Information Owners.** Information owners shall:
- 1.4.2.1. Maintain both the physical and logical security of the information technology resources and information under their jurisdiction.

- 1.4.2.2. Ensure the classification of data is defined and designated in a manner consistent with County data classifications.
- 1.4.2.3. Periodically conduct a risk assessment of each information technology resource for which they are responsible to determine both risks and vulnerabilities.
- 1.4.2.4. Ensure, for the information utilized, stored, and accessed by their departments, that security measures are implemented which are appropriate to the level of protection required by policy and law.
- 1.4.2.5. Maintain information access controls over department information. In the fields of physical security and information security, access control is the selective restriction of access to a place or other resource. The act of accessing may mean consuming, entering, or using. Permission to access a resource is called authorization.
- 1.4.3. **Director of Information Technology.** The Director of Information Technology shall:
 - 1.4.3.1. Establish and maintain County-wide information security policies.
 - 1.4.3.2. Act as the County's Change Control Agent. No changes to the County's information infrastructure shall be executed without the Change Control Agent's knowledge and approval.
 - 1.4.3.3. Maintain safeguards for the information technology resources and information under the Director of Information Technology's jurisdiction.
 - 1.4.3.4. Review and approve or deny exceptions to this Policy.
- 1.4.4. **Department of Information Technology.** The Department of Information Technology shall:
 - 1.4.4.1. Provide technical guidance to all County departments.
 - 1.4.4.2. Under the direction of the Chief Security and Privacy Officer, maintain a Security Incident Response Team to respond to virus infestations, hacker intrusions, and similar events.
 - 1.4.4.3. Review proposals for new services, hardware and software, networks, external connectivity, or other systems for communicating information for compliance with County Information Security Policy and Security Standards, and shall consult appropriate County businesses for business-specific regulatory requirements and applicable legal mandates.
 - 1.4.4.4. Review County participation in external networks, or as a provider of services that external parties rely on, for compliance with County Information Security Policy and Security Standards.
- 1.4.5. **Departmental Information Security Officers (ISOs).** Each Department Head, in coordination with the Chief Security and Privacy Officer, shall nominate an individual to serve as that Department's Information Security Officer. The Departmental Information Security Officer shall:
 - 1.4.5.1. Be a full time County employee.
 - 1.4.5.2. Not directly report to the Chief Security and Privacy Officer
 - 1.4.5.3. Collaborate with and coordinate departmental information protection actions with the Chief Security and Privacy Officer. The responsibilities of the Departmental Information Security Officers encompass all information for which the department has administrative responsibility. They are responsible for ensuring adherence to procedures, guidelines and safeguards that are required to protect information,

confidentiality and privacy rights, and to ensure integrity, auditability, and controllability of the information resources within the department.

- 1.4.5.4. Monitor departmental compliance with County Security Policy, County Security Standards, Information Security best practices, business-specific regulatory requirements, and applicable legal mandates, as applied to the particular business and/or mission of County departments.
 - 1.4.5.5. Secure and maintain the confidentiality and integrity of protected information within the department by reviewing all security considerations for the department's automated and manual processes in coordination with County Security Policy, County Privacy Policy, County Security Standards, Information Security best practices, business and/or mission-specific regulatory requirements, and applicable legal mandates.
 - 1.4.5.6. Work with the Chief Security and Privacy Officer and Information Security Staff to analyze department information environments on an ongoing basis to identify risks arising from changes in those environments.
 - 1.4.5.7. Serve as the initial security point of contact for their department's employees,
 - 1.4.5.8. Work with the County's Security Incident Response Team, report all Information Security incidents to the Chief Security and Privacy Officer, and investigate the authenticity of reported security violations in coordination with the Chief Security and Privacy Officer and the Security Incident Response Team before initiating corrective actions within their department.
- 1.4.6. **Department Managers and Supervisors.** Department Managers and Supervisors shall:
- 1.4.6.1. Ensure that employees under their supervision implement security measures as defined in County Security Policies and Standards and as appropriate to their data classifications.
 - 1.4.6.2. Inform employees under their supervision of information security issues and promote overall security awareness.
 - 1.4.6.3. Enforce compliance with County Information Security Policy and Information Security Standards.
 - 1.4.6.4. Conduct entry or pre-exit security clearance processes upon employment or termination of employment of officers or employees or fulfillment of contractual agreements.
- 1.4.7. **County Officers and employees.** All County Officers, employees and affiliates working for or doing business with the County shall:
- 1.4.7.1. Do no harm to nor attempt to harm or steal any County information resource or information resource.
 - 1.4.7.2. Know and follow County Policies and Standards, and apply best practices pertaining to protected information and information security.
 - 1.4.7.3. Prohibit unauthorized individuals from obtaining access to County information technology resources and information and access only the information for which he/she is authorized in the course of normal business activity.
 - 1.4.7.4. Maintain exclusive control over and use of his/her password or other authentication mechanism and protect it from inadvertent disclosure to others.

- 1.4.7.5. Ensure that information under his/her control and/or direction is safeguarded according to its data classification.
- 1.4.7.6. Report to his/her supervisor or Departmental Information Security Officer any incident that appears to compromise the security of County information resources.
- 1.4.7.7. Complete information security awareness training annually.

1.5. ACCEPTANCE OF RISK AND RESPONSIBILITY

- 1.5.1.1. The security of the County's information technology resources and information is the responsibility of all County employees.
- 1.5.1.2. Information security risk decisions are assigned to, and are the responsibility of the County departments whose information is the target of the particular risk. When presented with a Chief Security and Privacy Officer-directed or approved security risk assessment of an existing or proposed change or service, information owners shall review the risks to their information technology resources and information from the identified security risks and security gaps, and either:
 - 1.5.1.2.1. Accept the risks to their information ; or
 - 1.5.1.2.2. Execute Information Security's recommendations and/or other mitigation steps in order to reduce the risk to an acceptable level; or
 - 1.5.1.2.3. Transfer the risks as necessary.
- 1.5.1.3. The County Administrative Officer, their designee, and/or the County Board of Supervisors shall be responsible for any information or information technology resource risk decisions where the risk applies to a significant portion of the County or to the entire County as a whole.

1.6. STANDARDS

- 1.6.1. In addition to County Information Security Standards documents established and maintained by the Chief Security and Privacy Officer, the County shall adopt the ISO/IEC 27002 standard entitled "Information technology - Security techniques - Code of practice for information security management", a standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO/IEC 27002 provides best practice recommendations on information security management for use by those who are responsible for initiating, implementing or maintaining Information Security Management Systems.

1.7. ACCESS CONTROL

- 1.7.1. Access to County information technology resources and information shall be authorized by the information owners.
- 1.7.2. Wherever technically feasible, all access to information shall be granted according the National Institute of Standards and Technology's Role Based Access Control (RBAC) and Role Based Security models. With RBAC, security is managed at a level that corresponds closely to the organization's structure. Each user is assigned one or more roles, and each role is assigned one or more privileges that are permitted to users in that role. Security administration with RBAC consists of determining the operations that must be executed by persons in particular jobs, and assigning employees to the proper roles.
- 1.7.3. Every software program and every user of any County system or network shall operate using only privileges necessary to complete the job. The computer and communications system privileges of all users, systems, and software shall be restricted based on the need-to-know. Systems, files and user permissions shall begin in a closed state and shall

only be opened to those whose role requires access. Default access settings shall be configured for denial-of-access and opened thereafter as necessary to accomplish County business purposes.

1.7.4. Regarding Access Authorization:

- 1.7.4.1. Requests for new User IDs, role and privilege changes for County officers and employees shall be requested by the user's manager.
 - 1.7.4.2. Requests for new User IDs, role and privilege changes for individuals who are not County officers or employees shall be requested in writing by the department head or authorized representative sponsoring the work activity that necessitates access.
 - 1.7.4.3. All users shall sign a compliance statement indicating the user understands and agrees to abide by County Policies, Standards and procedures related to access to County computers and networks. Users must receive a copy of these policies, standards and procedures and sign that they have received these copies.
 - 1.7.4.4. Documentation reflecting user access requests and changes shall be retained for a period of at least one year.
 - 1.7.4.5. All user-IDs shall automatically have their associated privileges revoked after 30 days of inactivity. Automatic suspension shall include notification to the assigned department for information and recommendations.
 - 1.7.4.6. Privileges granted to users who are not County officers or employees shall be granted for periods of 90 days or less. As needed, users who are not County officers or employees shall have their privileges reauthorized by the sponsoring department head every 90 days.
- 1.7.5. All access rights and privileges granted to users shall be re-evaluated on an annual basis by management. In response to feedback from management, all access rights and privileges no longer needed by users shall be promptly revoked.

1.8. **AUDIT**

1.8.1. **Scope**

- 1.8.1.1. This policy applies to all County employees and affiliates. This covers all computer and communication devices owned or operated by the County. This also covers any computer and communications devices that are present on County premises or used for County business, but which may not be owned or operated by County. This also applies to any computing resource that accesses, stores or otherwise provides connectivity to County resources, including personal devices such as smart phones, tablets and laptops. Unless contractual agreements dictate otherwise, messages sent over County computer and communications systems are the property of the County. To properly protect and manage this property, management reserves the right to examine all information stored in or transmitted by these systems. County employees and personnel of affiliates shall have no expectation of privacy associated with the information they store in or send through these systems.

1.8.2. **Requirements**

- 1.8.2.1. Compliance with County Policies and Standards shall be regularly (not less than annually) audited by the Information Security Team. Audits may be conducted to:
 - 1.8.2.1.1. Ensure integrity, confidentiality, and availability of information and resources. Confidentiality is about protecting the information from disclosure to unauthorized parties. Integrity is protecting information from being modified by unauthorized parties. Availability refers to ensuring that authorized parties

are able to access the information when needed. For information specific to a particular department, this auditing task may be delegated to the department's Departmental Information Security Officer.

- 1.8.2.1.2. Investigate possible security incidents to ensure conformance to County security policies
 - 1.8.2.1.3. Monitor user or system activity where appropriate
 - 1.8.2.1.4. Verify that vulnerability management is being maintained at the appropriate security level
 - 1.8.2.1.5. Verify that malware and other system protections are being maintained at current levels
 - 1.8.2.1.6. Validate compliance with stated security policies.
- 1.8.2.2. All information technology resources throughout the County shall be accessible and auditable by the Chief Security and Privacy Officer per the details in section 1.4.1.13.1.

1.9. **COMPUTER SECURITY**

1.9.1. **DEFINITIONS**

- 1.9.1.1. Shareware – Shareware (also termed trialware or demoware) is proprietary software that is provided to users on a limited basis and sometimes only for certain limited trial basis and pursuant to a license which restricts any commercial benefit, use or exploitation of the software.
 - 1.9.1.2. Open Source Software – Open-source software (OSS) is computer software with its source code made available and licensed in such manner that the copyright holder provides the rights to study, change and distribute the software to anyone and for any purpose.
 - 1.9.1.3. Freeware - Freeware (a hybrid of "free" and "software") is software that is available for use at no monetary cost or for an optional fee, but usually (although not necessarily) closed source with one or more restricted usage rights.
- 1.9.2. County computers shall only be used in a secure environment. An environment is secure when appropriate controls have been established to protect computer software, hardware, and information. These controls shall provide a measure of protection commensurate with the classification of the data and the assessed risks.
- 1.9.3. Secure user identification and authentication shall be used on all devices, applications and systems software.
- 1.9.4. All County computing and network-connected devices shall utilize an access control system that provides privilege control as well as change control, and shall employ software which restricts access to the files of each user, logs the activities of each user, and has special privileges granted to a systems administrator. Portable computers and home computers which contain County information are also covered by this policy.
- 1.9.5. All County computing and network-connected devices shall be as fully protected as possible from malicious computer hacking and all forms of malware including computer viruses, worms, trojan horses, rootkits, bots, crimeware and all other malicious and unwanted software, including new types not listed here. These systems shall be regularly examined to assure their compliance with this policy.

- 1.9.6. All software running on devices connected to the County's network shall utilize the latest security updates provided by the software vendor or the County as addressed in County standards.
- 1.9.7. County computers and networks shall only run trusted software that has been approved by a Department Head or departmental Information Security Officer. Trusted software includes software from business partners, knowledgeable and trusted user groups, well-known systems security authorities (such as SANS), computer or network vendors, or commercial software vendors. Software downloaded from the Internet, shareware, open source software, freeware and other software from un-trusted sources shall not be used unless it has been approved in writing by the department's Information Security Officer and the Chief Security & Privacy Officer has been notified. In instances where concerns exist regarding the use of particular software, the Chief Security & Privacy Officer may require a formal risk assessment be completed. Users shall not download or install any unapproved software on any County device.
- 1.9.8. The use of a "personally-owned" computer or mobile computing device such as tablets, smartphones, etc., or any of its component parts to connect to the county network or access internal county resources shall be permitted only after permission has been granted by the employee's Departmental Information Security Officer (ISO) and the appropriate policy and acceptable use forms have been completed.
- 1.9.9. Buildings which house County information technology resources shall be protected with physical security measures that prevent unauthorized persons from gaining access to the equipment and that lessen the risks of theft, destruction, and/or misuse.
- 1.9.10. All County servers and network equipment shall be physically secured and be placed in locked cabinets, locked closets, or locked computer rooms.
- 1.9.11. The Information Technology Department shall create and maintain a list of managers who are authorized to control and grant access to County facilities that contain information technology resources.
- 1.9.12. County Departments shall maintain records of the persons currently and previously inside the non-public areas their facilities.
- 1.9.13. Inventory records of computer equipment shall be kept up-to-date. The master inventory shall be maintained by the Department of Information Technology, with the assistance of the individual departments, in conformance with the adopted Information Technology Resources Management policies.
- 1.9.14. The loss or theft of any computer hardware and/or software shall be reported as soon as practical to the department's Information Security Officer (ISO).

1.10. IDENTIFICATION AND AUTHENTICATION

- 1.10.1. All computers shall have, at minimum, password access controls that limit access to users with unique user ids and passwords.
- 1.10.2. Wherever technically possible, all County applications and services shall utilize a single centralized, single sign-on, identity management and authentication source.
- 1.10.3. Each user shall positively identify themselves as individuals with authorizations that are unique to each individual user.
 - 1.10.3.1. Generic, guest or universal IDs are not permitted without a signed acceptance of risk by the Department Head or designee.

- 1.10.4. Initial authentication assigned to new users or authentication (such as passwords) changed by third-party reset shall be changed by the user at the user's next login.
- 1.10.5. Default or vendor-supplied authentication (such as passwords) shall be changed before placed into production.
- 1.10.6. User authentication information (such as passwords) shall never be disclosed to or shared with anyone or be exposed in openly viewable form.
- 1.10.7. All changes of user-IDs shall be logged.
- 1.10.8. Passwords shall be long, complex, unpredictable and difficult to guess.
- 1.10.9. Passwords shall be regularly changed into non-identical and non-reused passwords.
- 1.10.10. Every log-in banner must include a special notice. This notice must state:
 - 1.10.10.1. The system is to be used only by authorized users.
 - 1.10.10.2. By continuing to use the system, the user represents that he/she is an authorized user.
 - 1.10.10.3. All activities on the system shall be monitored.
 - 1.10.10.4. Users shall have no expectation of privacy.
- 1.10.11. Systems and applications must not divulge information about the County or grant access to information until after a valid user login.

1.11. **SECURITY LOGGING**

- 1.11.1. Users shall be put on notice about the specific acts that constitute computer and network security violations. Users shall also be informed that such violations will be logged. Refer to the County's Appropriate Use Policy for more details.
- 1.11.2. County computer and communications systems shall securely log all significant security events. Security events include but are not limited to:
 - 1.11.2.1. Account logon events
 - 1.11.2.2. Account management
 - 1.11.2.3. Users switching user-IDs
 - 1.11.2.4. Password guessing attempts
 - 1.11.2.5. Changes to user privileges
 - 1.11.2.6. Electronic configuration policy changes
 - 1.11.2.7. Attempts to use unauthorized privileges
 - 1.11.2.8. Attempts to access unauthorized objects
 - 1.11.2.9. Modifications to production application software
 - 1.11.2.10. System events and modifications to system software
 - 1.11.2.11. Changes to logging subsystems
- 1.11.3. Logs containing security relevant events shall be securely retained by the Information Technology Department for at least three (3) months.
- 1.11.4. These logs shall be viewed daily and in a timely manner by assigned Server Administrators, Information Owners, or assigned Information Technology staff.

1.12. NETWORK SECURITY

1.12.1. Description

- 1.12.1.1. The County must comply with the requirements of the California Department of Justice, the requirements under FBI Criminal Justice Information System security policies, and the requirements of the California Law Enforcement Telecommunication System. As a result of these and other requirements, strict controls over the security of the County network are necessary.

1.12.2. Requirements

- 1.12.2.1. No changes to the County's data networks shall occur without the expressed knowledge and consent of the Information Technology Department.
- 1.12.2.2. New types of connections between two or more County computer systems or networks shall not be established unless such approval has first been obtained in writing from the Director of Information Technology.
- 1.12.2.3. The bridging of County networks or the participation in external networks as a provider of services that external parties rely upon shall be expressly prohibited unless explicitly permitted by the Director of Information Technology in writing. Bridging is defined as the simple act of using a computing device to create a connection between a foreign network and the local County network at the same time. Examples of "bridging of the County network" include, but are not limited to:
 - 1.12.2.3.1. Connecting a live modem to a network-connected County computer.
 - 1.12.2.3.2. Connecting a FAX machine to the County network.
 - 1.12.2.3.3. Connecting to a County computer from a remote location using means in violation of County Security Standards.
 - 1.12.2.3.4. Connecting from a County computer to a computer or network on the Internet using VPN or other remote control mechanisms in violation of County Security Standards.
 - 1.12.2.3.5. Connecting alternative access to the Internet to the County network or a network-connected County computer or device.
 - 1.12.2.3.6. Connecting the County network or a network-connected County computer to any third party network using means in violation of County Security Standards.
 - 1.12.2.3.7. Connecting a wireless device to the County network that concurrently is connected to a third party provider network
- 1.12.2.4. As processes deployed across a local or wide area network can result in a negative impact on overall network performance, controlled testing of network processes shall be conducted before being deployed. Processes that have negative impact on the network shall not be deployed until performance issues are coordinated and network performance issues have been addressed.

1.13. SECURITY PERIMETER

1.13.1. Purpose

- 1.13.1.1. This section establishes essential policies and operational requirements for Security Perimeter Architecture (the Security Perimeter).

1.13.2. **Scope**

- 1.13.2.1. This applies to all resources, systems, connectivity, and services as defined within the Security Perimeter and to all entities located on the County's Wide Area Network. Furthermore, it applies to all County employees, officers, and affiliates, including all personnel affiliated with third parties participating in any capacity within the County's defined Security Perimeter environment. Existing legal requirements shall not be superseded by this policy.

1.13.3. **Description**

- 1.13.3.1. The Security Perimeter is an essential and critical Wide Area Network component and is crucial to the security of County infrastructure and information systems. The Security Perimeter is defined as the "managed point of entry/exit" to County infrastructure resources. It includes but is not limited to all County Firewalls, Intrusion Prevention Systems, Public Service Networks (also referred to as Demilitarized Zones, or DMZ's), Virtual Private Networks (VPN), remote connectivity resources, and the network architecture resources providing connectivity for the environment.
- 1.13.3.2. This section defines the requirements which apply to components of the Security Perimeter; both the logical and physical. This does not replace or supersede overarching Security Policies which address overall development of network deployment, but rather focuses on critical components establishing the stability and security of the Security Perimeter.
- 1.13.3.3. The Security Perimeter is divided into two categories; its logical components and its physical components.

1.13.4. **Logical Components**

1.13.4.1. Definitions

- 1.13.4.1.1. Logical components refer to the logical representation of how the Security Perimeter is viewed, and include, but are not necessarily limited to:

- 1.13.4.1.1.1. Internet
- 1.13.4.1.1.2. Intranet: Connectivity of the security perimeter to the Intranet (the County's Wide Area Network, or WAN) provides County access to external resources foreign to the County's WAN.
- 1.13.4.1.1.3. Extranet: Connectivity to business partners, vendors, external connectivity to other private networks
- 1.13.4.1.1.4. Public Service Network (also called a De-militarized Zone, or DMZ): Secured zones that protect resources from full exposure to any connection (Internet, Extranet, Remote Access, Intranet, etc).
- 1.13.4.1.1.5. Remote Access: remote access connectivity such as dial-up networking and/or Virtual Private Networking (VPN) that is utilized to gain privileged access to County Infrastructure systems.

1.13.4.2. Applicable Policies

- 1.13.4.2.1.1. The point(s) of logical component connectivity shall be noted as such as well as be visually auditable.
- 1.13.4.2.1.2. Any logical perimeter component connections shall connect to a County firewall or similar security device and shall be managed by the Information Technology Department.

- 1.13.4.2.1.3. Where possible, disparate business partners or Extranets shall be secured and protected from each other
- 1.13.4.2.1.4. Where possible and appropriate, the network addresses of hosts and all other information not necessary to disclose shall be masked or hidden.
- 1.13.4.2.1.5. Placement of resources within a Public Service Network shall adhere to an established IT procedure.
- 1.13.4.2.1.6. Public Service Network hosted resources shall adhere to the requirements in County Information Security Standards.

1.13.5. Physical Components

1.13.5.1. Definitions

- 1.13.5.1.1.1. Firewalls: those devices which apply rules or filters to network traffic
- 1.13.5.1.1.2. Routers and Switches: those devices which provide connectivity and connections points to resources within the Security Perimeter
- 1.13.5.1.1.3. Remote Access Appliances: those devices which provide remote connectivity to County resources.
- 1.13.5.1.1.4. Circuits and Connectivity: provide access to foreign resources not part of the County's Wide Area Network. These most commonly include connections to the Internet and Extranet business partners.

1.13.5.2. Applicable Policies

- 1.13.5.2.1. Physical components, where capable and appropriate, shall be configured in such a manner as to not divulge their function and or location.
- 1.13.5.2.2. Physical components, where capable and appropriate, shall display warning banners for logon.
- 1.13.5.2.3. Physical component administrators shall have unique passwords and/or access methods.
- 1.13.5.2.4. Physical components shall be secured through physical and logical security measures allowing only authorized administrator access.
- 1.13.5.2.5. Physical components, where capable and appropriate, shall provide for auditing and logging.
- 1.13.5.2.6. Router(s) and Switch(es), where appropriate, shall leverage additional security functions such as Access Control Lists (ACL) that limit administrative access.
- 1.13.5.2.7. Unused ports shall remain in an inactive or shut state until required to be activated for connectivity.
- 1.13.5.2.8. All connections shall be clearly labeled and identifiable.
- 1.13.5.2.9. All connections shall physically be located in a sight or limited walking auditable radius.
- 1.13.5.2.10. All circuits shall terminate (county-side) on a County Router in the Information Technology department where possible.
- 1.13.5.2.11. Any circuits terminating (county-side) on an affiliate router shall then connect to a County managed Router or Firewall.

1.13.6. Management, Monitoring, and Control

- 1.13.6.1. This policy provision governs all resources which comprise the “management environment” of the County’s security perimeter. It refers to management consoles or any control device or method used to manage, control, or otherwise configure the security perimeter of the County. The following policies apply:
 - 1.13.6.1.1. All aspects of the County’s security perimeter shall be managed by the Information Technology Department.
 - 1.13.6.1.2. Only administrators authorized by the Director of Information Technology shall be granted access to management of the security perimeter.
 - 1.13.6.1.3. An auditable access and transaction history shall be available including logon, access, activities, and surveillance where appropriate.
 - 1.13.6.1.4. No changes to the security perimeter, including devices, systems and services placed on the County’s perimeter or in any Public Service Network shall occur without the written authorization of the Chief Security and Privacy Officer or IT Director.
- 1.13.6.2. No changes to the County’s defensive security posture, whether internal or on the security perimeter (including, but not limited to, changes to or the disabling of network firewalls, proxies, application firewalls, malicious website filtering) shall occur without the written authorization of the Chief Security and Privacy Officer or IT Director.

1.14. **REMOTE ACCESS**

1.14.1. **Scope**

- 1.14.1.1. This section applies to all County departments, officers, employees, and affiliates accessing the County network from a remote, non-County network-connected location. This applies to implementations of remote access directed through any type of remote access device or VPN Concentrator.

1.14.2. **Description**

- 1.14.2.1. Approved County employees and authorized third parties or affiliates (vendors, etc.) may use the benefits of County remote access. Users are responsible for selecting an Internet service provider (ISP), paying associated fees for these services, coordinating installation, and installing any required software in order to provide the appropriate levels of Internet connectivity so as to participate in the County’s remote access services. Additionally,
 - 1.14.2.1.1. All remote access devices enabling access to the County network shall be set up, configured and managed by the Department of Information Technology. All other remote access connections shall be strictly prohibited without the expressed written consent of the Director of Information Technology.
 - 1.14.2.1.2. All remote access connections must come through the Security Perimeter managed by the Information Technology Department.
 - 1.14.2.1.3. All County policies that apply to on-site individuals shall apply to individuals connecting remotely. All individuals are required to comply with County Security Policies and Security Standards whenever connecting to the County’s network or working with County information. Resources used to remotely connect to County networks and resources must adhere to the adopted Security Standards for County-connecting systems. Individuals utilizing

remote access are responsible for complying with the County's Security and Appropriate Use Policies and for the security of information at their remote work site.

- 1.14.2.1.4. By using remote access technology with personal or third party equipment, individuals understand that their machines are a de facto extension of the County's network and, as such, are subject to the same rules, regulations and legal discovery requirements that apply to County-owned equipment.
- 1.14.2.1.5. All County employees working remotely shall comply with any existing County Telecommuting Policies.
- 1.14.2.1.6. All remotely-connecting individuals shall be aware of the types and classifications of data they are working with and the legal, regulatory and policy requirements regarding the handling, transmission and storage of such data.
- 1.14.2.1.7. Users of computers connecting to the County's network shall configure their computers to comply with the County's Security Policies and Security Standards and shall actively protect the County's network from harm or intent to harm.
- 1.14.2.1.8. All remote access users shall ensure that unauthorized users are not allowed access to the County's networks.
- 1.14.2.1.9. Remote access sessions utilizing the Internet as the means of connectivity shall be encrypted.
- 1.14.2.1.10. Remote access shall be controlled using either a one-time password mechanism (such as a token device), or a public/private encryption key system with a strong passphrase and back-end authentication, or a similar, more secure method.
- 1.14.2.1.11. Remote access to County networks is limited to circumstances where access is required for legitimate business. In the case of County employees where remote access may be granted to the entire County network, two-factor authentication shall be utilized to gain access.
- 1.14.2.1.12. When actively connected to the County network, remote access devices shall force all traffic to and from the remote PC over the connection to the County. All other traffic will be dropped. Dual (split) tunneling shall not be permitted; only one network connection shall be allowed.
- 1.14.2.1.13. No bridging of the County's network to any other network shall be allowed at any time. Bridging is defined as the simple act of using a computing device to create a connection between a foreign network and the local County of Monterey network at the same time. County network resources are only available to the remotely connecting device via the authorized connection provided and shall never be shared with other devices and networks.
- 1.14.2.1.14. The use of modems is prohibited unless approved by the Director of Information Technology.
- 1.14.2.1.15. Approved modems that are utilized for vendor remote maintenance on County computer and communication systems shall be disabled until the specific time they are needed by the vendor. These ports shall be disabled after use. Alternatively, dial-up connections can be established with vendors via outbound calls initiated by County employees.

- 1.14.2.1.16. Remote access users shall be automatically disconnected from the County's network after 20 minutes of inactivity. Pings or other artificial network processes shall not be used to keep the connection open.
 - 1.14.2.1.17. Only approved remote access client software shall be used.
 - 1.14.2.1.18. Users shall not connect to the County network while using an unprotected or unauthorized wireless network, unless VPN is used.
 - 1.14.2.1.19. Remote access sessions shall be monitored and logged.
 - 1.14.2.1.20. All inter-processor commands from non-County locations are prohibited unless a user or process has first logged-in. Examples of such commands are remotely-initiated requests for a list of users within the County or a list of users logged on locally to a system.
- 1.14.2.2. The County has an unrestricted right of access to, and disclosure of, all information and software on any County equipment, or personal equipment used for County business or media, at the request of the appropriate County official(s). Information generated or placed into personally-owned personal computers being used on County time, as well as work undertaken on behalf of the County during or outside of any County worksite and/or work hours shall be made available for review at the request of appropriate County officials. For any applicable servicing, compliance auditing or forensics, this equipment shall be delivered to the County Information Technology facility or be made available through remote access. Such access and disclosure shall be in accordance with, and subject to any controls or restrictions imposed by applicable statutes or licenses.

1.15. **WIRELESS SECURITY**

1.15.1. **Purpose**

This section prohibits access to County networks by unsecured and unauthorized wireless communication mechanisms. Only wireless systems that meet the criteria of this policy, or that have been granted an exclusive waiver by the Director of Information Technology, are approved for connectivity to County networks.

1.15.2. **Scope**

This section covers all wireless information communication devices (e.g., personal computers, cellular phones, PDAs, tablet computers, etc.) connected to any County internal network. This includes any form of wireless communication device capable of transmitting information. Wireless devices and/or networks without connectivity to the County's networks do not fall under the purview of this policy.

1.15.3. **Description**

1.15.3.1. Wireless implementations shall:

- 1.15.3.1.1. Be pre-approved by the Information Technology Department.
- 1.15.3.1.2. Be compliant with the Information Technology Department's wireless architecture
- 1.15.3.1.3. Be managed by and within the Information Technology Department's wireless architecture.
- 1.15.3.1.4. Comply with all County Information Security Standards.

- 1.15.4. Devices using non-County wireless services (such as cell phone networks) shall not be used for information transmissions containing County protected information unless the connection is encrypted. Likewise, other broadcast networking technologies--such radio-based local area networks--shall not be used to transmit County protected information unless the link or the information itself is encrypted.

1.16. **PROTECTED INFORMATION**

1.16.1. **Purpose**

- 1.16.1.1. To establish policy for the handling, storage and destruction of protected County electronic information.

1.16.2. **Scope**

- 1.16.2.1. The information covered in this section includes, but is not limited to, information that is either stored or shared electronically by any means.
- 1.16.2.2. All employees shall familiarize themselves with the information labeling and handling principles that follow. The principle behind an information protection policy is that only the intended audience or authorized individuals should see or have an opportunity to see information and only authorized individuals should be able to modify information. Exceptions to this principle are made only by those who have the authority to do so.
- 1.16.2.3. For the purposes of this policy, all information is categorized into two main classifications:
 - 1.16.2.3.1. Public information. Public information is defined as any information that can be made available to the public via the California Public Records act.
 - 1.16.2.3.2. Protected information. Protected information is any information not declared by law or policy to be public information. Protected information includes the following, as defined by County policies and California and federal laws and regulations, as may be amended from time to time:
 - 1.16.2.3.2.1. Personally Identifiable Information
 - 1.16.2.3.2.2. Protected Health Information
 - 1.16.2.3.2.3. Protected Criminal Justice Information
 - 1.16.2.3.2.4. Protected Critical Infrastructure Information
 - 1.16.2.3.2.5. Intellectual Property

1.16.3. **Description**

- 1.16.3.1. Protected Information
 - 1.16.3.1.1. Protected information and media shall be suitably marked with the highest relevant sensitivity classification.
 - 1.16.3.1.2. Access should only be granted to those individuals (County employees and affiliates) designated with approved access.
 - 1.16.3.1.3. Electronic distribution within the County must be marked as "Confidential". Electronic distribution outside of the County must be encrypted securely.
 - 1.16.3.1.4. Storage

- 1.16.3.1.4.1. Protected information shall be kept from view of unauthorized people. Access to work areas containing protected information shall be physically restricted. Visitor access to work areas containing protected information shall be controlled by guards, receptionists, or other staff.
- 1.16.3.1.4.2. Printers that are printing protected information shall not be left unattended until the protected printouts are removed.
- 1.16.3.1.4.3. Protected information should not be stored or displayed on machines without physical and software access controls.
- 1.16.3.1.4.4. All information storage media (such as hard disk drives, USB sticks, magnetic tapes, CD-ROMs, etc.) shall be encrypted and physically secured when not in use.
- 1.16.3.1.4.5. Any medium for backup/recovery shall have the same or better access and security controls as the original information.
- 1.16.3.1.4.6. Protected information shall not be stored in a given location any longer than the business function or law requires.
- 1.16.3.1.4.7. Protected information transferred to laptops, PDA's and all other portable media shall be encrypted. These laptops, PDA's and all other portable media shall remain in the possession of the traveler at all times (not be checked in).
- 1.16.3.1.4.8. Equipment that is no longer under the physical control of the County shall have protected information expunged/cleared prior to transferring control to an outside agency (e.g. surplus, sending equipment out for repair, loaning equipment, etc.). Alternatively, repair vendors shall execute a nondisclosure agreement with the County.
- 1.16.3.1.4.9. Individual access controls are required for protected electronic information.
- 1.16.3.1.4.10. Individual access controls for physical security are required for all forms of storage.
- 1.16.3.1.5. Disposal/Destruction:
 - 1.16.3.1.5.1. Electronic information shall be expunged/cleared or zeroed.
 - 1.16.3.1.5.2. Media shall be reliably electronically erased or physically destroyed.
- 1.16.3.2. The penalty for deliberate or inadvertent disclosure includes discipline, up to and including termination of employment and possible civil and/or criminal prosecution.
- 1.16.4. **Security Controls**
 - 1.16.4.1. Information about security measures utilized for County computer and communication systems is confidential and shall not be released to anyone without written permission from the Director of Information Technology or the Chief Security and Privacy Officer.
 - 1.16.4.2. As permitted by the California Public Records Act, the County shall not disclose information security records of a public agency if, on the facts of the particular case, disclosure of those records would reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of a public agency.
- 1.16.5. **Encryption keys**

Encryption keys used for County information are classified as protected information. Access is limited to those who have responsibility for the management of those keys. Encryption keys shall not be revealed to consultants, contractors, temporaries, or third parties without the written approval of the Chief Security and Privacy Officer. Likewise, encryption keys shall always be encrypted when transmitted over any network.

1.16.6. Encryption responsibilities

- 1.16.6.1. When providing computer networking services, the County does not provide default message protection services such as encryption. Accordingly, no responsibility is assumed for the disclosure of information sent over the County's networks, and no assurances are made about the privacy of information handled by the County internal networks. In those instances where encryption or other special controls are required, it is the information owner's responsibility to make sure that adequate security precautions have been taken. However, nothing in this section should be construed to imply that County policy does not support the controls dictated by agreements with third parties (such as organizations which have entrusted the County with confidential information).
- 1.16.6.2. Whenever such facilities are commercially available, the County shall employ automated rather than manual encryption key management processes for the protection of information on County networks.

1.17. SECURITY INCIDENT RESPONSE

1.17.1. Purpose

- 1.17.1.1. The County will follow established policies and procedures to address indications that the security of the County's information technology resources may have been compromised. Such procedures include ensuring that the appropriate level of County management becomes involved in determining the response to an information technology security incident.

1.17.2. Description

1.17.2.1. Security Incident Definition

Security Incidents include, but are not limited to:

- 1.17.2.1.1. Actions apparently intended to harm or illegally access County information resources or information.
- 1.17.2.1.2. Potential violations of Federal law, State law, Business-specific Regulations or County Policy involving a County information technology resource or information.
- 1.17.2.1.3. A breach, attempted breach or other unauthorized access of a County information technology resource or information. The incident may originate from the County network or an outside entity.
- 1.17.2.1.4. Attempts (either failed or successful) to gain unauthorized access to a system or its information.
- 1.17.2.1.5. The infection of any County system with a worm, Trojan horse, rootkit, bot, crimeware, virus, or other types of malware.

- 1.17.2.1.6. Conduct using, in whole or in part, a County information technology resource or information which could be construed as harassing, or in violation of County Policies.
- 1.17.2.1.7. Action or attempt to utilize, alter or degrade a County owned or operated information technology resource in a manner inconsistent with County policies.
- 1.17.2.1.8. Unwanted disruption or denial of service against County information technology resource or information.
- 1.17.2.1.9. The unauthorized use of an information technology resource or information.
- 1.17.2.1.10. Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

1.17.3. Security Incident Response Team

The Chief Security and Privacy Officer shall maintain a Security Incident Response Team consisting of individuals from many disciplines, trained to respond to major security incidents. The members shall be equipped with the tools and understanding of security incident response processes and procedures, work through closed means of communication, and shall maintain confidentiality.

1.17.4. Incident Reporting

- 1.17.4.1. Employees and affiliates shall promptly notify the Departmental Information Security Officer when:
 - 1.17.4.1.1. Intrusion attempts, security breaches, theft or loss of hardware and other security related incidents have been perpetrated against the County
 - 1.17.4.1.2. There is knowledge or a reasonable suspicion of an incident which violates the confidentiality, integrity, or availability of information.
 - 1.17.4.1.3. A virus, worm, bot, rootkit or other malware has been discovered
 - 1.17.4.1.4. It is unclear whether a situation should be considered a Security Incident
- 1.17.4.2. Departmental Information Security Officers shall notify the ITD Information Security Team of all but minor information security incidents.
- 1.17.4.3. Security Incidents involving possible violation of Federal or California law shall be reported to the County's Chief Security and Privacy Officer.
- 1.17.4.4. Incident Reports shall include:
 - 1.17.4.4.1. A description of events
 - 1.17.4.4.2. Approximate timelines
 - 1.17.4.4.3. Parties involved
 - 1.17.4.4.4. Resolution of the incident (if any)
 - 1.17.4.4.5. External notifications required

1.17.5. Incident Escalation

- 1.17.5.1. Upon notification of an incident, the County's Chief Security and Privacy Officer or designee shall, as needed, escalate the incident to the County's Security Incident Response Team.

1.17.5.2. If activated, the County's Security Incident Response Team shall plan and coordinate the activities of all departments involved, keeping other concerned departments advised. In carrying out this responsibility, the County's Security Incident Response Team shall ensure that operational decisions are elevated to the levels of County government required to protect the interests of the County and others impacted by the incident. Such decisions include, but are not limited to:

- 1.17.5.2.1. Restricting information system access or operations to protect against further information disclosure
- 1.17.5.2.2. Involving law enforcement agencies in cases where applicable statutes appear to have been violated

1.17.5.3. The Chief Security and Privacy Officer or designee shall document the deliberations, decisions, and actions of the County's Security Incident Response Team.

1.17.5.4. All external notification, reporting or publicizing shall be approved by the Department Head or the Director of Information Technology.

1.17.6. **Incident Actions**

1.17.6.1. If the incident appears to involve a compromised computer system, the state of the computer system shall not be altered. The computer system shall remain turned on, all currently running computer programs shall be left as is, and the computer shall not be used until directed otherwise by the County's Incident Response team.

1.17.6.2. Whenever system security has been compromised or if there is a convincing reason to believe that it has been compromised:

- 1.17.6.2.1. All passwords residing on the system or entered on the system shall be immediately changed by the person responsible for the account.
- 1.17.6.2.2. A trusted version of the operating system and all security-related software shall be reloaded from trusted storage media such as CD-ROMs or original installation media.
- 1.17.6.2.3. All changes to user privileges taking effect since the time of suspected system compromise shall be immediately reviewed by the systems administrator for unauthorized modifications.

1.18. **TERMINATION OF EMPLOYMENT**

1.18.1. **Purpose**

1.18.1.1. This section identifies methods to effectively limit and remove access to information resources for both voluntary and involuntary terminations within the County organization.

1.18.2. **Scope**

1.18.2.1. This applies to all County employees and affiliates regardless of pay scale.

1.18.3. **Description**

1.18.3.1. **Voluntary separation/termination**

- 1.18.3.1.1. Since terminations can be expected regularly, utilizing an *Employee Separation/Termination Checklist* for outgoing or transferring employees, as part of standard HR "out-processing" ensures that system user accounts are removed in a timely manner. It normally includes:

- 1.18.3.1.1.1. Removal of access privileges, computer accounts, authentication tokens.
- 1.18.3.1.1.2. Control of keys.
- 1.18.3.1.1.3. Briefing on the continuing responsibility for confidentiality and privacy.
- 1.18.3.1.1.4. Return of property.
- 1.18.3.1.1.5. Verifying that files and information under the user's control are available or transferred to the department.

1.18.3.2. **Involuntary Termination**

- 1.18.3.2.1. In addition to the process identified for voluntary separation/termination, involuntary terminations shall include:
 - 1.18.3.2.1.1. Terminating access as quickly as possible, preferably at the same time (or just before) the employee is notified of his/her dismissal.
 - 1.18.3.2.1.2. If possible during the "notice of termination" period, assign the individual to a restricted area to function, particularly where employees are capable of changing programs or modifying systems or applications.
 - 1.18.3.2.1.3. Any time termination involves persons in a position of trust such as a systems administrator, the County shall have a replacement administrator chosen and ready to assume their duties as soon as possible.

1.18.3.3. **Termination Process**

- 1.18.3.3.1. In the event that an employee, consultant, or contractor is terminating his or her relationship with the County, the individual's immediate management is responsible for ensuring all property in the custody of the individual is returned, that the Information Technology Department is given prompt notification by utilization of a Termination/Separation Checklist in order to revoke all computer access rights for that individual, that administrators handling the computer accounts used by the individual are notified, and that all other work-related privileges of the employee are terminated.
- 1.18.3.3.2. Upon notification of an employee's termination from employment at the County, the following shall be accomplished:
 - 1.18.3.3.2.1. The department manager or designee shall notify the Information Technology Department and complete a *Termination/Separation Checklist*.
 - 1.18.3.3.2.2. The department manager or designee shall notify those departments in which the employee, consultant, or contractor had access through keys, tokens, or access cards so that access privileges can be deactivated.
 - 1.18.3.3.2.3. A copy of the *Termination/Separation Checklist* will be forwarded to the Information Technology Department. Following the guidelines outlined in the checklist and the separation date, the Information Technology Department shall:
 - 1.18.3.3.2.3.1. Ensure the individual's account(s) have been disabled.
 - 1.18.3.3.2.3.2. Ensure the individual's access to standalone applications (those where access is not controlled by a central account) have been disabled.

- 1.18.3.3.2.3.3. Ensure the individual's name has been removed from any internal system access lists, authentication server lists, firewall lists, etc.
 - 1.18.3.3.2.3.4. Change any network passwords the individual may have had access to (to include routers, firewalls, etc.).
 - 1.18.3.3.2.3.5. Terminate the individual's access to unique County information technology resources. Change passwords if necessary.
 - 1.18.3.3.2.3.6. Terminate remote access account(s) and access tokens (if applicable).
 - 1.18.3.3.2.3.7. Assign access rights over the individual's files and directories.
 - 1.18.3.3.2.3.8. Re-route email to the appropriate person identified by department management (if applicable).
 - 1.18.3.3.2.3.9. When applicable, perform a general security scan of the system(s) for any unknown back doors, etc.
- 1.18.3.3.3. On or near the last day of employment or association with the County, the department manager or designee shall meet with the individual to receive identification materials, keys, tokens or access cards used to permit access to County networks and facilities. Access to non-public areas of facilities shall be cancelled upon termination of an employment relationship with the County and all physical security access codes known by the individual deactivated or changed.
 - 1.18.3.3.4. In the event the individual has County equipment off-site, this equipment shall be turned over to the department manager or designee and forwarded to the Information Technology Department during the last scheduled day of employment or other association with the County.
 - 1.18.3.3.5. The individual shall be asked to read and sign a non-disclosure agreement intended to protect confidential and private information.
 - 1.18.3.3.6. Documentation of items received and a copy of the termination/separation checklist shall be kept in the individual's permanent record of employment/association with the County.
 - 1.18.3.3.7.** All inactive user accounts shall be removed from County systems after a ninety (90) day period.

1.19. **EXCEPTIONS**

Under rare circumstances, the County may need to vary from these policies. All such instances shall be approved in writing and in advance by the Director of Information Technology and/or the Chief Security and Privacy Officer. Disputed issues may be escalated to the Information Technology Governance Committee for final decision as necessary.

1.20. **ENFORCEMENT**

Violators of this policy may be subject to appropriate disciplinary action up to and including employment termination, termination of agreements, denial of services, and/or legal penalties, both criminal and civil.

Monterey County



Subject: [Appropriate Use Policy](#)
Date Issued: May 13, 2014
Issued by: Information Technology Governance Committee
Approved by: The County of Monterey Board of Supervisors
Applies to: All County Officials, Employees and Affiliates

2. INFORMATION TECHNOLOGY APPROPRIATE USE POLICY

2.1.1. POLICY PURPOSE

- 2.1.1.1. This policy outlines permissible use of information technology equipment and information resources in the County. It governs the conduct of persons granted the privilege of access to County information technology resources, whether at a County facility or elsewhere, and refers to all information resources whether individually controlled or shared, standalone or networked.
- 2.1.1.2. This policy is intended to facilitate access for County officials, employees, affiliates, and constituents to both internal and external information and to promote accomplishment of the objectives of the project or task(s) for which access was granted. It is intended, also, to avoid inappropriate, illegal or unauthorized use of information technology equipment or resources. Uses inconsistent with this policy may subject violators to sanctions, as specified below.

2.1.2. DEFINITIONS

- 2.1.2.1. Affiliates – Includes, but is not limited to, third party contractors, volunteers, advisory and other committee and commission members, vendors, or others associated with the County in order to accomplish County business.
- 2.1.2.2. Broadcast – the initiation and/or distribution of a message, unrelated to the accomplishment of County business, over an information technology Resource to all devices and users attached to the resource, which has not been directed to a specific subset of devices or users when the technology resource allows the sender of the message to select narrower distribution.
- 2.1.2.3. Chain E-Mail – Any message, unrelated to the accomplishment of County business, sent to one or more people that asks the recipient to forward it to multiple others.
- 2.1.2.4. Information Technology Resources – Any information in electronic or audiovisual format or any hardware or software that make possible the storage and use of such information, including electronic mail, local

databases, externally accessed databases, CD-ROM, motion picture film, recorded magnetic media, photographs, and any other digitized information.

- 2.1.2.5. Network – Workstations and connections of computer workstations to servers or any other computer system through a local or wide area network, Internet, Intranet, or modem connection.

2.1.3. **GENERAL POLICY REQUIREMENTS**

- 2.1.3.1. All computer information created utilizing County computing resources is the property of the County.
- 2.1.3.2. All computer use, including Internet use, on County networks shall be monitored.
- 2.1.3.3. Persons granted access to County computing resources shall not:
 - 2.1.3.3.1. Make copies of any software, information, communication, data, digital media, or other information technology Resource without specific authorization.
 - 2.1.3.3.2. Utilize, allow or request others to utilize County information technology equipment or resources, or confidential information acquired through the use of those resources or equipment, for personal benefit or any other purpose unrelated to the accomplishment of County business.
 - 2.1.3.3.3. Except in the authorized conduct of their work assignment, divulge the contents of any record or report to any person, or provide information about, or lists of, County employees to parties outside the County.
 - 2.1.3.3.4. Knowingly include, or cause to be included, in any record or report a false, intentionally inaccurate, or misleading entry or knowingly alter an existing database, document, or digitized data with false and/or unauthorized information.
 - 2.1.3.3.5. Divulge authentication information or passwords to anyone.
 - 2.1.3.3.6. Provide access to information technology equipment and resources to any individual that is not properly authorized to access them.
 - 2.1.3.3.7. Destroy, alter, dismantle, or disfigure the County's information equipment, technologies, properties, or facilities, including those owned by third parties.
 - 2.1.3.3.8. Modify County information technology equipment, systems files, or software, install software on any County equipment without specific authorization, or change computer information without being the data owner or having authority to change that information.
 - 2.1.3.3.9. Send electronic communications which hide the identity of the sender or misrepresent the sender as someone else.
 - 2.1.3.3.10. Use County information technology equipment or resources in violation of any County policy or local, state, or federal law including but not limited to policies and laws governing privacy, public record, copyright or patent.

2.1.4. **System and Network Activities**

Persons granted access to County computing resources shall not:

- 2.1.4.1.1. Copy or use software without an appropriate license or right to use.

- 2.1.4.1.2. Use products on County equipment that are not licensed for use by the County or which violate the rights of any person or organization protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software.
- 2.1.4.1.3. Reproduce copyrighted material including, but not limited to, digitization, copying or distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, copyrighted digital media files, or install copyrighted software for which the County or the user does not have an active license.
- 2.1.4.1.4. Remove information technology equipment, system files, or software programs from County premises, unless specifically authorized by department management.
- 2.1.4.1.5. Play computer games in the County workplace, with the exception of computer games for the purpose of training first-time users on mouse, pointer, or stylus control while the user is in a formal training mode.
- 2.1.4.1.6. Export software, technical information, encryption software, or technology in violation of international or regional export control laws. Users shall consult with appropriate management prior to exporting any material that is in question.
- 2.1.4.1.7. Introduce malicious programs into the County network or any County computing device (e.g., viruses, worms, Trojan horses, root kits, e-mail bombs, etc.).
- 2.1.4.2. **Offensive behavior**
 - Persons granted access to County computing resources shall not:
 - 2.1.4.2.1. Use County information technology equipment or resources to engage in procuring or transmitting material in violation of sexual harassment or hostile workplace law.
 - 2.1.4.2.2. Send messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, ethnicity, political affiliation, physical attributes, or sexual orientation.
 - 2.1.4.2.3. Transmit, retrieve, or store any communications of a discriminatory or harassing nature or materials that may be perceived as obscene, unless directly related to the conduct of law enforcement activities or investigations.
 - 2.1.4.2.4. Transmit, retrieve, or store abusive, profane, or offensive language or pictures (including all pornography) on the County's network unless required by business necessity (e.g. investigative case evidence) and authorized in writing by department directive.
 - 2.1.4.2.5. Make fraudulent offers of products, items, or services.
 - 2.1.4.2.6. Transmit, retrieve, or store illegal material, such as child pornography, from any source, with the singular exception of job requirements related to the fulfillment of law enforcement responsibilities.
- 2.1.4.3. **Testing and circumvention of security controls**

- 2.1.4.3.1. For purposes of this section, "testing and circumvention" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- 2.1.4.3.2. Unless approved in advance in writing by the Chief Security and Privacy Officer and performed in coordination with Information Security, persons granted access to County computing resources shall not :
 - 2.1.4.3.2.1. Access data of which the user is not an intended recipient.
 - 2.1.4.3.2.2. Log in to a system or account that the user is not expressly authorized to access.
 - 2.1.4.3.2.3. Test, circumvent, or attempt to compromise computer or communication system security measures.
 - 2.1.4.3.2.4. Use network security scanning or vulnerability assessment tools. This includes the use of such tools for network testing and/or troubleshooting.
 - 2.1.4.3.2.5. Engage in system cracking (hacking), password cracking (guessing), port scanning, security scanning, or similar attempts to compromise security measures.
 - 2.1.4.3.2.6. Use short-cuts bypassing systems security measures, or engage in pranks and practical jokes involving the compromise of systems security measures.
 - 2.1.4.3.2.7. Execute any form of network monitoring that will intercept data not intended for the user.
 - 2.1.4.3.2.8. Test or circumvent, or attempt to compromise user authentication or security of any host, network, or account.
 - 2.1.4.3.2.9. Interfere with or deny service to any user other than the user's host (e.g., denial of service attack).
 - 2.1.4.3.2.10. Use any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable a user's session, via any means.
 - 2.1.4.3.2.11. Utilize any form of network sniffer device or software or configuring sniffing ports on the County's network.

2.1.5. Electronic Mail (e-mail) and Internet Use

- 2.1.5.1. E-mail and Internet access are tools provided to accomplish County business. With the exception described below, private or personal use of e-mail and Internet access unrelated to County business is prohibited.
 - 2.1.5.1.1. Infrequent, brief personal use of e-mail and Internet access is permissible only where it is of such a limited nature that it does not interfere with performance of duties, does not detract from responsiveness to the public, does not result in cost to the County, and does not compromise the security or integrity of County information technology equipment or resources. Ordinarily, such use should occur, if at all, before or after work hours and during employee breaks. Examples of permitted personal use include transmitting e-mail to a family member to assure safe arrival home, confirming health care appointments, or checking traffic conditions for a commute. Examples of prohibited personal use

include online shopping, making personal vacation plans, private postings on blogs, chat rooms and social media sites, and instant messaging.

- 2.1.5.1.2. Departments may adopt more stringent policy regarding personal use of email and Internet access in order to serve their specific business needs and County functions. Individual Department policy, if any, should be consulted for specific guidance.
- 2.1.5.2. All e-mail and Internet records transmitted over the County network are County records and shall be transmitted only to individuals who have a business need to receive them. Users shall have no expectation of privacy in personal or business communications over County computers or networks, including fax machines and networked copiers.
- 2.1.5.3. All messages communicated on the County's e-mail system shall contain the name of the actual sender.
- 2.1.5.4. Any messages or information sent to another individual or entity outside of the County shall not disclose any confidential or proprietary information to parties with no County business reason to know.
- 2.1.5.5. County officers, employees and affiliates shall not broadcast e-mail messages to all users without specific authorization by the Department Head or Division Chief. Authorized messages with broad distribution shall minimize the size of the message, limit the size and number of attachments, and restrict the use of embedded images. Any announcement which any user wishes to make utilizing County email that is not strictly related to County business shall be approved in advance by his or her department manager and must be of general interest to County employees as determined by the Department Head or Division Chief.
- 2.1.5.6. The County's e-mail system may be made available for use by County employees for official union or Association related business, subject to applicable law and regulations, the conditions set forth in this policy, and any agreed upon limitations regarding use. Use is subject to prior written agreement between the Union or Association and the County. Employees using the County's e-mail network for such purposes shall be required to familiarize themselves with and abide by these requirements. Use of the system for union business is restricted in that there shall be:
 - 2.1.5.6.1. No union or Association related messages may be broadcast.
 - 2.1.5.6.2. No confidential or individual-specific information may be communicated, such as information regarding a disciplinary action.
 - 2.1.5.6.3. No messages that might malign the County, its employees, or officials.
 - 2.1.5.6.4. No messages may be used to coordinate any job actions.
- 2.1.5.7. Sending unsolicited e-mail messages shall be prohibited, including but not limited to the following examples:
 - 2.1.5.7.1. The sending of "junk mail" or other advertising material to individuals who did not specifically request such material (i.e. e-mail spam).
 - 2.1.5.7.2. Any form of illegal harassment.
 - 2.1.5.7.3. Forging of e-mail header information.

2.1.5.7.4. The sending or forwarding of chain e-mail. County officers, employees and affiliates are directed to break the chain, deleting any chain email messages received and requesting the sender to discontinue forwarding mail of this type.

2.1.6. Telecommunications Equipment Use

2.1.6.1. Electronic voice communications via telephones, radios, pagers, cell phones, images transmitted via facsimile machines, computers or tablets transmitting audio files as a means of voice communication, and any other related technologies shall be subject to County policy and regulation. It is the responsibility of the person initiating any telecommunication transmission utilizing County information technology resources to ensure that the communication complies with County policy and regulation.

2.1.7. Individual County Departments may define "conditions of use" for more restrictive access to County information technology resources when additional detail, guidelines, and/or restrictions are consistent with this policy and necessary for achievement of the department's mission, goals, objectives, or functions.

2.2. EXCEPTIONS

Under rare circumstances, the County may need to vary from these policies. All such instances shall be approved in writing and in advance by the Director of Information Technology and/or the Chief Security and Privacy Officer. Disputed issues may be escalated to the Information Technology Governance Committee for final decision as necessary.

2.3. ENFORCEMENT

Violators of this policy may be subject to disciplinary action up to and including employment termination, termination of agreements, denial of service, loss of access privileges, and/or additional legal penalties, both criminal and civil. Allegations of violations of Equal Employment Opportunity protections will be referred to the Office of Equal Employment Opportunity for investigation. Reports or complaints of possible illegal material will be investigated by the Department having ownership of the information resources used with consultation from the Information Technology Department, County Counsel, and/or other agencies as appropriate.

Monterey County



Subject: Data Privacy Policy
Date Issued: May 13, 2014
Issued by: Information Technology Governance Committee
Approved by: The County of Monterey Board of Supervisors
Applies to: All County Officials, Employees and Affiliates

3. DATA PRIVACY POLICY

3.1. POLICY PURPOSE

To establish practices for protecting the privacy of personal and/or Personally Identifiable Information that may be collected through the use of the County's information technology resources.

3.2. POLICY SCOPE

This policy applies to all County officials, employees and affiliates.

3.3. DEFINITIONS

- 3.3.1. Affiliates – Includes but is not limited to, third party contractors, volunteers, advisory and other committee and commission members, vendors, or others associated with the County in order to accomplish County business.
- 3.3.2. Cookies – a piece of text describing user preferences and choices, typically stored in a small file on the user's computer hard drive as a result of accessing a web site and interacting with it via web browser software.
- 3.3.3. Personally Identifiable Information (PII) – personal data that includes names, identification numbers (social security numbers, driver's license numbers, account names, passwords, etc.), post and e-mail addresses, phone and facsimile numbers, billing information, medical records, vehicle information such as vehicle identifications numbers, and complaint information.

3.4. POLICY DESCRIPTION

- 3.4.1. Monterey County and its departments shall implement data privacy and confidentiality practices that meet the requirements of state and federal legislation and regulation, as they may be amended and supplemented from time to time, including (but not necessarily limited to) the following laws:

- 3.4.1.1. Lanterman-Petris-Short Act (LPS) of 1969

- 3.4.1.2. The Fair Credit Reporting Act (1970)
- 3.4.1.3. Privacy Act of 1974
- 3.4.1.4. Family Education Rights and Privacy Act (1974)
- 3.4.1.5. Right to Financial Privacy (1978)
- 3.4.1.6. Confidentiality of Medical Information Act (CMIA) of 1979
- 3.4.1.7. Privacy Protection Act of 1980
- 3.4.1.8. Cable Communications Policy Act of 1984
- 3.4.1.9. Electronic Communications Privacy Act (1986)
- 3.4.1.10. Patient Access to Health Records Act (PAHRA) of 1988
- 3.4.1.11. Driver's Privacy Protection Act of 1994
- 3.4.1.12. Communications Assistance for Law Enforcement Act of 1994
- 3.4.1.13. Telecommunications Act of 1996
- 3.4.1.14. Health Insurance Portability and Accountability Act (HIPAA) of 1996
- 3.4.1.15. Children's Online Privacy Protection Act (COPPA) of 1998
- 3.4.1.16. Financial Modernization Act (Graham-Leach=Bliley Act) (2000)
- 3.4.1.17. USA Patriot Act (2001)
- 3.4.1.18. SB 1386, the California Information Practices Act (2003)
- 3.4.1.19. The Payment Card Industry Data Security Standard (PCI DSS) (2004)
- 3.4.1.20. Patient Safety and Quality Improvement Act (2005)
- 3.4.1.21. DHCS Medical Data Privacy & Security Agreement (2007)
- 3.4.1.22. Genetic Information Nondiscrimination Act (GINA) 2008
- 3.4.1.23. Health Information and Technology for Economic and Clinical Health Act (HITECT) of 2009
- 3.4.1.24. Red Flag Program Clarification Act (2010)
- 3.4.2. County officials, employees, affiliates or others with access to PII through the County's information technology resources shall abide by this policy, hold any such information in confidence, and shall not use such information for any purpose other than to carry out the County business purpose they are charged with performing.
- 3.4.3. Monterey County shall not sell, rent, or lease PII to third parties. The County shall not share any PII with any outside party without first ensuring that the outside party has similar privacy policies in place. Exceptions include the following situations:
 - 3.4.3.1. Sharing the information, on an expedited basis, is in the vital interests of the subject of that information or some other person (e.g., health care information).
 - 3.4.3.2. Sharing the information is necessary to carry out law enforcement duties and responsibilities.
 - 3.4.3.3. Sharing the information is necessary for the establishment of a legal claim or defense.

- 3.4.3.4. Sharing the information is related to the provision of medical care or diagnosis.
- 3.4.3.5. The subject of the information has consented to sharing the information with third parties.
- 3.4.3.6. The information has been unambiguously made public by the subject of that information.
- 3.4.3.7. The information is mandated to be made available to qualified third parties by law or code (e.g., California State Elections Code).

3.4.4. Posting the Privacy Policy

- 3.4.4.1. County Departments shall post a summary privacy policy as it specifically applies to the information handled by their department. This should include providing notice as to what personal information is collected, used, and disclosed; what choices persons conducting business with the County have with regard to the business collection, use, and disclosure of that information; what access the public or others will have to that information; what security measures are taken to protect the information, and what enforcement and redress mechanisms are in place to remedy any violations of this policy.

3.4.5. Provide Adequate Security to Maintain Privacy

- 3.4.5.1. County Departments shall take all reasonable steps to ensure that PII is safe from unauthorized access, either physical or electronic. These steps will include at least the following:
 - 3.4.5.1.1. Maintain logs to properly track information and assure that data is only accessed by individuals authorized by the department.
 - 3.4.5.1.2. Perform at least an annual review of its written data security policies.
 - 3.4.5.1.3. Assure that officers, employees, affiliates and those with access to PII are properly trained on maintaining confidentiality.
 - 3.4.5.1.4. Store any such information in a secure environment (using features such as locks and electronic security).
- 3.4.5.2. County Departments shall use levels of encryption and authentication specified in the County's Information Security Standards for the transfer or receipt of health care information, social security numbers, financial transaction information (for example, a credit card number), or other sensitive or personally-identifiable information.
- 3.4.5.3. County Departments shall provide industry standard levels of security and integrity to protect data maintained on their computers, and shall contractually require all third parties and affiliates to provide and maintain similar and appropriate levels of security.

3.4.6. Respect Preferences Regarding Unsolicited E-Mail

- 3.4.6.1. County Departments shall enable those persons who do not wish to be contacted online with a means to opt out from future communications via electronic mail and shall maintain a "Do not contact" list.

3.4.7. Access and Correction

- 3.4.7.1. Any County Department that collects PII shall implement and maintain a process under which the collected information may be reviewed and factual

inaccuracies corrected upon request. The process shall include a means to authenticate the identity of an individual that requests access or correction. If review and/or correction are prohibited by law, an explanation of the prohibition shall be provided to authenticated individuals and a contact for further information will be provided, as well as a reference to the County's Information Technology Data Privacy Policy.

3.4.8. Computer Tracking and Cookies

- 3.4.8.1. The County web site shall not be designed or constructed to track, collect, or distribute personal information not specifically entered by visitors. Site logs may be used to generate certain kinds of non-identifying site usage data, such as the number of hits and visits to County sites. This information may be used for internal purposes by technical support staff to provide better services to the public and may also be provided to others; however the statistics shall contain no personally-identifiable information.
- 3.4.8.2. The County may use non-identifying cookies in support of easier web site navigation and access to forms. County web sites shall be designed to support access and use even if the user's browser is set to reject cookies. Cookies shall not be used to generate personal data, shall not read personal data from the user's machine, and shall not be connected to anything that could be used to identify the user.

3.5. **EXCEPTIONS**

Under rare circumstances, the County may need to vary from these policies. All such instances shall be approved in writing and in advance by the Director of Information Technology and/or the Chief Security and Privacy Officer. Disputed issues may be escalated to the Information Technology Governance Committee for final decision as necessary.

3.6. **ENFORCEMENT**

Violators of this policy may be subject to disciplinary action up to and including employment termination, termination of agreements, denial of service, and/or legal penalties, both criminal and civil. Similarly, contractors, affiliates and other third parties may be liable to a complaining party or the County for damages or penalties and to the County for indemnification and claim defense costs.

Monterey County



Subject: Social Media Usage Policy
Date Issued: May 13, 2014
Issued by: Information Technology Governance Committee
Approved by: The County of Monterey Board of Supervisors
Applies to: All County Officials, Employees and Affiliates

4. Social Media Usage Policy

4.1. PURPOSE

4.1.1. Departments may opt to utilize social media sites to reach a broader, Internet audience in order to deliver public information and customer service. In order to ensure against potential dissemination of inaccurate information, departments shall follow the policies stated below.

4.2. POLICY

- 4.2.1. Only Social Media sites that have been approved by the Department Heads and are listed in County Information Security Standards may be used to post content.
- 4.2.2. Social media sites do not replace departments' websites as their primary Internet presence. Thus, content posted to departmental social media sites shall contain links directing users back to the department's official website for in-depth information, forms, documents or online services necessary to conduct business with the County.
- 4.2.3. In using social media sites, departments shall comply with County policies and guidelines, including but not limited to:
 - 4.2.3.1. Security Policy
 - 4.2.3.2. Appropriate Use Policy
 - 4.2.3.3. Data Privacy Policy
 - 4.2.3.4. Internal departmental policies
- 4.2.4. Departments are responsible for ensuring their social media content is accurate and up-to-date.
- 4.2.5. Departments will adopt a method to monitor all changes or updates to social media content by:
 - 4.2.5.1. Implementing an approved, automated tool to monitor social media sites to eliminate malicious modifications or,
 - 4.2.5.2. If an approved automated tool does not exist, manually monitoring social media sites as often as possible.
 - 4.2.5.3. Departments must submit a Social Networking Website Utilization Agreement, signed by the Department head, indicating the manner in which the social media site will be monitored.
- 4.2.6. Departments are responsible for ensuring social media content that they post complies with applicable Federal, State and County laws, regulations and policies. This includes

adherence to established laws and policies regarding copyright, records retention, and privacy.

- 4.2.7. Information on County social media sites shall be limited to official postings by the departments. The departments, however, may include an email link or other contact information on social media pages that allow the public to communicate with departments.
- 4.2.8. Because social media sites are mechanisms to provide information to the public, postings that contain any of the following are not allowed:
 - 4.2.8.1. Comments not relevant to the topic(s) communicated;
 - 4.2.8.2. Comments in support of or opposition to political campaigns or ballot measures;
 - 4.2.8.3. Profane language or content;
 - 4.2.8.4. Content that promotes, fosters, or perpetuates discrimination on the basis of race, creed, color, age, religion, gender, marital status, status with regard to public assistance, national origin, physical or mental disability or sexual orientation;
 - 4.2.8.5. Sexual content or links to sexual content;
 - 4.2.8.6. Conduct or encouragement of illegal activity;
 - 4.2.8.7. Information that may tend to compromise the safety or security of the public or public systems;
 - 4.2.8.8. Content that violates a legal ownership interest of any other party.
- 4.2.9. The County Administrative Office reserves the right to restrict or remove any content that is deemed in violation of this social media policy or any applicable law.
- 4.2.10. For each social media site approved for use by the County's Information Security Officers, the following documentation will be developed and adopted by departments:
 - 4.2.10.1. Operational and use guidelines
 - 4.2.10.2. Standards and processes for managing accounts on social media sites
 - 4.2.10.3. Standards for the administration of social media sites
 - 4.2.10.4. Action plan to respond in the event the department's social media site is compromised
- 4.2.11. Departments shall add a disclaimer that alerts the public that they are no longer on a County site and that the social media site's privacy policy applies.
- 4.2.12. Applications on social media sites should not be used unless doing so serves a County business purpose, adds to the user experience, and comes from a trusted source. The County may deny access to or removal of an application at any time if there is significant reason to think it is compromising the security of County resources.

Exhibit A: Social Networking Utilization Agreement

The _____ (department/agency) will comply with the requirements defined in the Monterey County Social Media Use Policy for our information posted on _____ (Facebook, Twitter, etc)

The webpage will be automatically monitored using _____ (tool and version). The tool logs will be checked by members of Department staff. Unauthorized modification will be corrected upon detection and the Public Information Office will be notified.

Currently automated tools are not available to monitor this site. Members of Department staff have been assigned to manually monitor the content on my department's webpage. It will be checked ____ times a day and the results logged. Unauthorized modification will be corrected upon detection and the Public Information Office will be notified. When an automated tool becomes available for this site, it will be installed and incorporated in our process.

Department Head: _____ Date: _____


Agency Head: _____ Date: _____

CERTIFICATION REGARDING LOBBYING

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 any 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 document for sub-awards at all tiers (including sub-contracts, sub-grants, and contracts under grants, loans, and cooperative agreements, and that all sub-recipients shall certify and disclose accordingly.

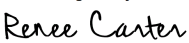
This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by Section 1352, Title 31, U.S. Code. Any person who fails to 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.

<p>DocuSigned by:  Signature</p>	<p>President and CEO Title</p>
<p>SolutionsWest Agency/Organization</p>	<p>8/30/2023 10:08 AM PDT Date</p>

CHILD ABUSE & NEGLECT REPORTING CERTIFICATION

CONTRACTOR hereby acknowledges that this contract for services will bring CONTRACTOR in contact with children, and that CONTRACTOR has received from COUNTY a copy of Penal Code Sections 11165.7 and 11166 as required by the Child Abuse and Neglect Reporting Act (Penal Code Sections 11164, et seq). CONTRACTOR further certifies that it has knowledge of the provisions of the Act, and will comply with its provisions, which define a mandated reporter and requires that reports of child abuse or neglect be made by a mandated reporter whenever, in his or her professional capacity or within the scope of his or her employment, he/she has knowledge or observes a child whom he/she knows or reasonably suspects has been a victim of neglect or abuse.

CONTRACTOR further gives assurance that all of its employees, consultants, and agents performing services under this Agreement, who are mandated reporters under the Act, sign statements indicating that they know of, and will comply with, the Act's reporting requirements.

DocuSigned by:

Authorized Signature

8/30/2023 | 10:08 AM PDT

Date

- ◆ 24-hour Bilingual Child Abuse Hotline 1-800-606-6618
- ◆ Mandated Child Abuse Reporter Training is available, at no cost, through the Child Abuse Prevention Council of Monterey County (CAPC), 755-4737.

EXHIBIT I


**ELDER/DEPENDENT ADULT
ABUSE & NEGLECT REPORTING
CERTIFICATION**

CONTRACTOR hereby acknowledges that this contract for services will bring CONTRACTOR in contact with dependent adults or elders, and that CONTRACTOR has received from COUNTY a copy of Welfare & Institutions Code Section 15659 as required by the Elder Abuse and Dependent Adult Civil Protection Act (Welfare & Institutions Code Sections 15600, et seq). CONTRACTOR certifies that it has knowledge of the provisions of the Act, and will comply with its provisions which define a mandated reporter, and requires that reports of abuse or neglect be made by a mandated reporter when, in his or her professional capacity, or within the scope of his or her employment, he/she observes or has knowledge of an incident that reasonably appears to be physical abuse, abandonment, isolation, financial abuse, or neglect.

Form SOC 341, Report of Suspected Dependent Adult/Elder Abuse, and General Instructions are available on the California Department of Social Services website: <http://www.dss.cahwnet.gov/cdssweb/entres/forms/English/SOC341.pdf>

CONTRACTOR further gives assurance that all of its employees, consultants, and agents performing services under this Agreement, who are mandated reporters under the Act, sign statements indicating that they know of and will comply with the Act's reporting requirements.

Form SOC 341A, Statement Acknowledging Requirement to Report Suspected Abuse of Dependent Adult and Elders, is available on the California Department of Social Services website: <http://www.dss.cahwnet.gov/cdssweb/entres/forms/English/SOC341A.pdf>

DocuSigned by:

Authorized Signature

8/30/2023 | 10:08 AM PDT
Date

To Report Suspected Dependent Adult/Elder Abuse during regular business hours, call **1 (800) 510-2020**
To Report Suspected Dependent Adult/Elder Abuse after hours, call **911**

EXHIBIT I

WELFARE AND INSTITUTIONS CODE
SECTION 15659

15659.

- (a) Any person who enters into employment on or after January 1, 1995, as a care custodian, health practitioner, or with an adult protective services agency or a local law enforcement agency, prior to commencing his or her employment and as a prerequisite to that employment shall sign a statement on a form, that shall be provided by the prospective employer, to the effect that he or she has knowledge of Section 15630 and will comply with its provisions. The signed statement shall be retained by the employer.
- (b) Agencies or facilities that employ persons required to make reports pursuant to Section 15630, who were employed prior to January 1, 1995, shall inform those persons of their responsibility to make reports by delivering to them a copy of the statement specified in subdivision (a).
- (c) The cost of printing, distribution, and filing of these statements shall be borne by the employer.
- (d) On and after January 1, 1995, when a person is issued a state license or certificate to engage in a profession or occupation the members of which are required to make a report pursuant to Section 15630, the state agency issuing the license or certificate shall send a statement substantially similar to the one contained in subdivision (a) to the person at the same time as it transmits the document indicating licensure or certification to the person.
- (e) As an alternative to the procedure required by subdivision (d), a state agency may cause the required statement to be printed on all application forms for a license or certificate printed on or after January 1, 1995.
- (f) The retention of statements required by subdivision (a), and the delivery of statements required by subdivision (b) shall be the full extent of the employer's duty pursuant to this section. The failure of any employee or other person associated with the employer to report abuse of elders or dependent adults pursuant to Section 15630 or otherwise meet the requirements of this chapter shall be the sole responsibility of that person. The employer or facility shall incur no civil or other liability for the failure of these persons to comply with the requirements of this chapter.