FIRST AMENDMENT TO AGREEMENT BETWEEN THE COUNTY OF SANTA CLARA AND OIR GROUP FOR CORRECTION AND LAW ENFORCEMENT MONITORING SERVICES

The Agreement for Services (Agreement) by and between the County of Santa Clara (County) and OIR Group (Contractor) for the performance of correction and law enforcement monitoring services effective January 15, 2020, is amended as set forth below, effective February 1, 2024.

1. Section 1, regarding Nature of Services, is hereby deleted and replaced with the following:

1. Nature of Services

Consistent with Ordinance Code sections A20-61 *et seq.* and Board Policy 3.64, Contractor will perform the functions of the Office of Correction and Law Enforcement Monitoring, including by providing correction and law enforcement monitoring services to the County.

(a) Monitoring Services. Contractor will provide independent monitoring of, and reporting about, the Sheriff's Office and other agencies/departments involved in law enforcement, jail operations, jail facilities, as well as the employees and contractors involved with law enforcement and jail operations, including the provision of health services in the jails, as set forth in Ordinance Code sections A20-61 through A20-66. Monitoring services shall include, but are not limited to, the following:

i. Monitoring Sheriff's Office jail and law enforcement operations, the conditions of confinement in the jails, the provision of health services in the jails, the use of force in the jails and in law enforcement operations, compliance with civil rights laws, and the Sheriff's Office's response to inmate and public complaints related to law enforcement, jail operations, or conditions of confinement, including the provision of services to inmates and the conduct of employees, contractors, volunteers, and others who provide such services.

ii. Monitoring that includes matters relevant to Custody Health Services policies and procedures, as well as policies of the Santa Clara Valley Medical Center and Behavioral Health Services Department, that directly affect the medical and behavioral assessment and treatment of inmates. Such monitoring may also include examination of the timeliness of all business operations that have a direct impact on the operations of the jails provided by other County departments.

iii. Consistent with Government Code section 25303, reviewing and making recommendations regarding policies and best practices of the Office of the District Attorney and the Office of the Public Defender that have an

impact on jail or law enforcement operations. Such monitoring may include, but is not limited to, the effect of District Attorney and Public Defender policies and practices on the timeliness of criminal proceedings and the population of the jails.

iv. Periodically reviewing Sheriff's Office use of force patterns, trends, and statistics, the Sheriff's investigations of use of force incidents and allegations of misconduct, and Sheriff's Office disciplinary decisions. As it pertains to uniformed personnel, Contractor shall monitor and review investigations of incidents involving, but not limited to: any shooting involving uniformed personnel, whether duty-related or not; any in-custody death; any duty-related incident during which, or as a result of which, a person dies or suffers serious bodily injury; any incident, whether or not duty-related, in which uniformed personnel are under investigation for, or charged with, homicide, assault, kidnapping, or unlawful sexual behavior; or any incident, whether duty-related or not, in which uniformed personnel are under investigation for, or are charged by any jurisdiction with, a crime or violation in which a use of force or threatened use of force is an element of the offense.

v. As it pertains to Custody Health Services, monitoring and reviewing investigations of incidents involving: any in-custody death; any duty-related incident during which, or as a result of which, anyone dies or suffers serious bodily injury; or any serious neglect of inmates as it pertains to their mental and physical health.

vi. Reviewing the quality of audits and inspections conducted by the Sheriff's Office, and conducting its own periodic audits and inspections of the Sheriff's Office consistent with professional guidelines for the conduct of such audits. Such audits and inspections should supplement, not supplant, internal auditing and monitoring conducted by the Sheriff's Office.

vii. Investigating specific incidents involving Sheriff's Office personnel when requested by, or with the authorization of, the Sheriff or the Chief of Correction.

viii. Investigating specific incidents involving Custody Health Services consistent with the Board-approved work plan when requested by the Board or the County Executive.

(b) Other Duties. In addition to the monitoring services described above, Contractor will perform all other duties of the Office of Correction and Law Enforcement Monitoring as set forth in Ordinance Code sections A20-61 through A20-66, A20-9, A22-36, A40-8, and A6-281 through A6-285, including but not limited to:

i. Regularly conducting research and making policy recommendations to the Board of Supervisors, the Sheriff, and the County Executive as determined by a Board-approved work plan.

ii. Regularly communicating with the public, the Board of Supervisors, the Sheriff's Office, the District Attorney, the Public Defender, and the County Executive regarding the operations of the Sheriff's Office.

iii. Prior to each annual review of existing military-style equipment and any consideration by the Board of a military equipment use policy, conducting an analysis and advising the Board whether the existing or proposed military equipment, and the use policies governing that equipment, are effective and comport with modern policy and nationwide best practices.

iv. Assisting the Chief Privacy Officer and the Office of the County Counsel in vetting surveillance technologies used specifically for law enforcement and jail-related purposes pursuant to the County's Surveillance-Technology and Community-Safety Ordinance.

v. Cooperating in the establishment and operations of the Community Correction and Law Enforcement Monitoring Committee (Committee), including by nominating four members for consideration by the Board of Supervisors, attending and participating in Committee meetings, considering the advice and recommendations of the Committee regarding matters within the Contractor's scope of work, and providing input and staff assistance to the Committee.

2. Section 2, regarding Monitoring and Reporting Process, is hereby deleted and replaced with the following:

2. <u>Monitoring and Reporting Process</u>

Contractor shall perform its duties under this Agreement in accordance with the processes outlined below.

(a) <u>Annual Work Plan</u>. Contractor shall annually prioritize issues that it believes should be monitored, policies that it believes the Board should consider, and other duties to be performed consistent with Ordinance Code sections A20-61 through A20-66 and A6-281 through A6-285. These priorities shall be identified in an annual work plan approved by the Board. The work plan shall also discuss how Contractor intends its work to support mission alignment relating to law enforcement and jail operations and ensuring that the Board's goals and the purposes of the Office of Correction and Law Enforcement Monitoring, as described in Ordinance Code Section A2-61, are met.

Each annual work plan shall also include proposed performance standards for the Board's consideration. In conjunction with approving each annual work plan, the Board will adopt performance measures for that year's work.

A proposed work plan for the first year of the Agreement must be presented to the Public Safety and Justice Committee at its regularly scheduled meeting in April 2020. The Public Safety and Justice Committee will provide input and make a recommendation to the full Board so that the Board can approve the work plan at a regularly scheduled meeting in May 2020.

Work plans for subsequent years must be presented to Public Safety and Justice Committee at its regularly scheduled October or November meeting. The Public Safety and Justice Committee will provide input and make a recommendation to the full Board so that the Board can approve the work plan before the end of the calendar year.

(b) Reporting. The annual work plan shall address anticipated reports to the Board, other County agencies, and the public. Contractor shall report to the Board on its activities at least quarterly. In addition, Contractor shall provide at least one public, annual report each November. Contractor shall also report to the Board regarding any impediments to its ability to successfully perform its duties. The Public Safety and Justice Committee may recommend additional reporting to be included in the annual work plan or on an ad-hoc basis if additional reporting is necessitated due to urgent or significant matters subject to Contractor's monitoring. Contractor's reports may be public or confidential, as appropriate, but shall favor transparency to the public in accordance with applicable law and relevant provisions of this Agreement, including this Section 2(b), Section 9 (Coordination with County Counsel), Section 10 (Confidentiality), Section 20 (Compliance with the Health Insurance Portability and Accountability Act (HIPAA)), and Exhibit C (Business Associate Agreement).

In its annual report, Contractor shall report on its adherence to the performance standards adopted by the Board. The annual report shall also describe how Contractor's work contributes to the overall effectiveness of the criminal justice system, including but not limited to reducing recidivism, enhancing public safety, and furthering the safety of staff.

Unless otherwise directed by County Counsel, if a report contains findings, conclusions, or recommendations relating to the Sheriff's Office or any other County department, Contractor must provide a draft of the report to that department, following or concurrent with County Counsel review, and provide the department with a reasonable opportunity to review and seek correction of any inaccuracies before the report is finalized and to provide a response or other comment to be included in the report.

Before any report is finalized or made public, it must be reviewed by County Counsel to ensure compliance with state and federal confidentiality laws and other legal obligations. If County Counsel determines that a report contains information that could expose the County to legal liability or violate confidentiality requirements, County

Counsel will work with the Contractor to finalize the report and provide it confidentially to the Board. When a report is provided confidentially to the Board, County Counsel will work with Contractor, where feasible, to prepare a public version of the report omitting confidential and privileged information.

(c) Advisory Function. Contractor's role is solely advisory. Contractor has no authority to exercise supervisory oversight, impose discipline, or otherwise manage or direct the operations of any department or entity subject to its monitoring. Contractor shall not interfere with the independent investigatory or prosecutorial authority of the Sheriff or the District Attorney, or with the duties of the Public Defender imposed by the rules of professional conduct. Any questions or concerns regarding Contractor's role vis-à-vis the Sheriff, the District Attorney, or the Public Defender must be brought promptly to the attention of the County Counsel.

(d) Independence. Contractor must perform its monitoring and reporting functions in accordance with applicable governmental auditing standards. Contractor and its staff shall maintain the highest standards of independence, impartiality, and personal integrity in performing work under this Agreement. If Contractor becomes aware of any potential or actual conflict of interest or other matter that could impair its independence and impartiality, it must inform County Counsel immediately.

3. Section 3, regarding Term of Agreement, is hereby deleted and replaced with the following:

3. Term of Agreement

(a) This Agreement is effective from January 15, 2020 through January 14, 2030, unless terminated earlier pursuant to Section 5, or otherwise amended by the Board of Supervisors.

(b) If any reports included in the annual work plan or otherwise requested by the County are not completed upon the termination of this Agreement, the term of the Agreement may be extended by the parties' written mutual consent. Any extension by the parties under this provision must not increase County's obligation to compensate Contractor as set forth in the Section 4 of this Agreement.

4. Section 4, regarding Compensation and Billing, is hereby deleted and replaced with the following:

4. Compensation and Billing

(a) The County agrees to pay, and Contractor agrees to accept, payment according to the rate schedule below as full compensation for performance of tasks under this Agreement for the first year of this agreement. For subsequent years, including any optional years, the rates below may be adjusted effective January 15th, based on the percentage change in the annual Consumer Price Index (CPI) for the San Francisco-

Oakland-Hayward Region. The percentage change must be computed based on the change in the October CPI from the prior year October value to the most recent October value. However, the maximum annual adjustment to the prior year rates shall not exceed five percent per year.

Team Member	**Billing Rate/Hour**
Michael Gennaco	$250.00
Stephen Connolly	$250.00
Julie Ruhlin	$250.00
Teresa Magula	$250.00
Margo Frasier	$250.00
Dr. David Hellerstein	$385.00
Kimberly Pearson	$275.00
Karen Rea	$275.00
Kevin Kuykendall	$165.00
Howard Jordan	$250.00
Kate Eves	$220.00
Stacey Nelson	$250.00
Flo Finkle	$250.00
Brian Corr	$250.00
Samara Marion	$250.00
Office Administrator	$65.00

Contractor represents and warrants that it normally bills these rates for Contractor's services.

Pursuant to Section 24, upon the prior approval of the Board of Supervisors, Contractor may subcontract with additional persons to perform services under this Agreement. Contractor shall be compensated by the County for services performed by such persons at rates approved by the Board, not to exceed each such person's customary billing rate per hour.

(b) The County will reimburse actual, reasonable, and necessary out-of-pocket expenses incurred by Contractor, excluding telephone, facsimile, and postage charges. If accompanied by detailed receipts, travel expenses shall be reimbursed pursuant to the County's Travel Policy, which is incorporated into this Agreement by reference.

(c) Travel Time: Contractor will not be reimbursed for travel time to or from Santa Clara County. Contractor will be reimbursed up to a maximum of .50 hours per day for travel time within the Santa Clara County boundaries. All allowed travel time is to be billed at one-half of the applicable hourly rate.

(d) Total compensation and expenses for this Agreement shall not exceed $7,553,554.44 (Agreed Amount). Contractor shall notify the County when the total amount billed and the estimated amount of work in progress total 75 percent of the

Agreed Amount. The County shall not be responsible for any services or costs exceeding the Agreed Amount.

(e) Under no circumstances will Contractor receive any benefits or compensation not expressly described in this Agreement or any subsequent amendment. The only compensation received under this Agreement will be through payment of hourly rates and reimbursable expenses as set forth in this Section.

(f) Contractor shall submit monthly invoices itemized by date, name of the person providing the services, hours worked, and description of services. All invoices will have a Net 30-day payment term from the date of receipt and approval of correct and proper invoices. Payment is deemed to have been made on the date the County mails the warrant or initiates the electronic fund transfer.

5. Section 9, regarding Coordination with County Counsel, is hereby deleted and replaced with the following:

9. <u>Coordination with County Counsel</u>

(a) Contractor's work under this Agreement is likely to raise significant legal issues and may implicate potential legal liability for the County. Contractor is expected to work closely with County Counsel and shall immediately bring to County Counsel's attention any legal issues or matters implicating potential liability for the County or its employees.

(b) In performing its work under this Agreement, Contractor may have access to confidential communications and documents, including information obtained from inmates and members of the public, medical and mental health records, peace officer personnel records, and other confidential or privileged materials. Consistent with Section 10 of this Agreement, Contractor must work with County Counsel to ensure it understands and preserves the confidentiality of such documents and communications as required by state and federal law.

(c) Pursuant to Ordinance Code section A20-64(d), Contractor may issue a subpoena or subpoena duces tecum to the Sheriff, or to any officer or employee appointed by the Sheriff, under specified circumstances. If Contractor believes it may be necessary issue a subpoena, Contractor shall consult with County Counsel and may issue a subpoena only with the advice and approval of County Counsel.

(d) Through its monitoring functions, Contractor may discover matters that have the potential to expose the County to claims, litigation, administrative or compliance action, or criminal charges against the County or a County employee. All such matters must be reported immediately to County Counsel. Contractor shall not report on or communicate about such matters with any other person within or outside the County except pursuant to the direction and guidance of County Counsel. County Counsel will work with Contractor to ensure that potential liability can be appropriately addressed and

confidentiality appropriately maintained, while also providing the greatest possible degree of transparency to the public.

(e) It shall be the responsibility of County Counsel to determine whether any issue, matter, or communication raises legal concerns or could expose the County to legal liability. Contractor is not retained to provide, and shall not provide, legal advice.

6. Section 10, regarding Confidentiality, is hereby deleted and replaced with the following:

10. Confidentiality

(a) Intent. In performing services under this Agreement, Contractor is tasked simultaneously with assisting the County in its efforts to improve transparency and accountability and with safeguarding confidential and sensitive information. The monitoring services Contractor is required to provide under this Agreement necessarily involve disclosure to Contractor of detailed information about the County and individuals it serves, including information that may be protected from public disclosure by confidentiality laws, the attorney-client privilege, and/or other provisions of law that govern the nature and timing of disclosure of public information. Contractor understands that, in order for the Board to fully utilize Contractor's services to provide independent monitoring and reporting, members of the public, inmates, and County staff alike must feel confident that such information will be handled appropriately. Contractor agrees to comply with the confidentiality provisions of this Agreement and of applicable federal, state, and local laws, and Contractor will work closely with County Counsel to determine the scope of its confidentiality obligations.

(b) Information-Sharing. Contractor, in consultation with County Counsel, shall establish written protocols with the Sheriff's Office and the County Executive regarding access to, maintenance of, and disclosure of confidential information. The written protocols must be reviewed and approved by County Counsel pursuant to Ordinance Code section A20-64(b).

(c) Release of Information. Prior to the public release of any report or other information related to Contractor's work under this Agreement, Contractor must work with County Counsel to ensure the report or information can be made public in a manner that comports with Contractor's obligation to maintain the strictest confidentiality of certain protected information. Contractor may not disclose draft reports or information obtained by Contractor in the course of its work under this Agreement, nor identify or disclose any issues relating to its work under this Agreement, without the specific consent of the County, unless expressly permitted by this Agreement. Draft reports, information obtained by Contractor in the course of its monitoring, or issues relating to its monitoring or reporting efforts, may be provided on a need-to-know basis only to persons authorized by law or regulation to receive it, to County Counsel, and to such County department or agency heads who may have a business need to know in order to provide necessary information to the Contractor required for its monitoring and reporting functions. Should Contractor believe other release of information is required or warranted, Contractor shall

notify the County Counsel, who shall provide guidance and/or bring the issue to the attention of the Contract Liaison or Board as appropriate.

(d) Protected Health Information. Contractor may obtain and use Protected Health Information only pursuant to the terms of the Business Associated Agreement incorporated as Exhibit C to this Agreement.

Protected Health Information means any information, whether oral or recorded in any form or medium: (1) that relates to the past, present, or future physical or mental condition of an individual; the provision of health to an individual; or the past, present, or future payment for the provision of health care to an individual; (2) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under the HIPAA Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.103, and/or (3) identifies the individual (e.g. name, social security number, finger prints, photograph, or similar information) or with respect to which there is a reasonable basis to believe the information can be used to identify the individual either directly or by reference to other publicly available information. Protected Health Information includes Electronic Protected Health Information (45 C.F.R. § 160.103; 42 C.F.R. § 2.11).

(e) Employee and Investigative Records. With certain exceptions, County employee information and investigative/prosecutorial files of the Sheriff and District Attorney are confidential. Contractor must work with County Counsel to determine which employee records, including but not limited to peace officer records, and investigative information are confidential.

(f) Court Orders. In the event that Contractor receives a subpoena, court order, or other legal document requiring release of the information, or is informed that such a document is being requested, Contractor shall immediately give notice to the County Counsel, as described in Section 25, below, in sufficient time to permit the County to seek a protective order or other similar order.

(g) Use of Information. Information obtained and/or prepared by Contractor in the course of its work under this Contract is work product which is the property of the County. Should there be a request by any other party for the provision of such information, the determination of whether such documents or information should be provided to the requester must be made by the County.

(h) Scope. Contractor will be performing work and occupying office space in County facilities. In the course of its work, Contractor may obtain, encounter, or have access to confidential information unrelated to its monitoring duties. Contractor's confidentiality obligations extend to all confidential County information it obtains, encounters, or has access to, regardless of whether the confidential information is related to work performed under this Agreement. Contractor shall not disclose any confidential information related to the County except as specifically provided in this Agreement.

(i) Breach. Any breach by Contractor of the requirements of this Section constitutes a material breach of this Agreement. Contractor must ensure that any person assigned by Contractor to perform services under this Agreement, or any employee or subcontractor allowed by Contractor to have access to any information related to performance of services under this Agreement, is aware of and abides by the provisions of this Section.

7. Section 12, regarding Access to Documents, is hereby deleted and replaced with the following:

12. Access to Documents

At no charge to Contractor, County will furnish to Contractor any records, data, and other information which are, in the opinion of the County, necessary for the performance of this Agreement. Contractor will not remove originals of any official documents from the Board's offices or any other County office. County will provide timely access to staff and records as required by Contractor in fulfillment of the assignments pursuant to this Agreement. Contractor is permitted to store documents on its computers or the County's shared drives provided Contractor complies with relevant provisions of this Agreement, including but not limited to Section 10 (Confidentiality), Section 11 (County Data), Section 20 (Compliance With The Health Insurance Portability and Accountability Act (HIPAA)), Section 33 (ISO Security and Compliance Language), Section 34 (County Information Technology User Responsibility), and Section 35 (Remote Access). Notwithstanding the foregoing, County may require documents or data to be accessed and stored only on County systems or equipment when necessary for purposes of data security or confidentiality.

8. Section 21, regarding Conflicts of Interest, is hereby deleted and replaced with the following:

21. Conflicts of Interest; Political Reform Act

Contractor shall comply, and require its subcontractors to comply, with all (1) applicable requirements governing avoidance of impermissible client conflicts; and (2) federal, state and local conflict of interest and disclosure laws and regulations including, without limitation, California Government Code section 1090 et seq., the California Political Reform Act (California Government Code section 87100 et seq.) and the regulations of the Fair Political Practices Commission concerning disclosure and disqualification (2 California Code of Regulations section 18700 et seq.). Failure to do so constitutes a material breach of this Agreement and is grounds for immediate termination of this Agreement by the County.

In accepting this Agreement, Contractor covenants that it presently has no interest, and will not acquire any interest, direct or indirect, financial or otherwise, which would conflict in any manner or degree with the performance of this Agreement and any matter undertaken pursuant to this Agreement. Contractor further covenants that, in the

performance of this Agreement, it will not use any contractor or employ any person having such an interest. Contractor, including but not limited to Contractor's employees, agents, and subcontractors, may be subject to the disclosure and disqualification provisions of the California Political Reform Act of 1974 (the "Act"), that (1) requires such persons to disclose economic interests that may foreseeably be materially affected by the work performed under this Agreement, and (2) prohibits such persons from making or participating in making decisions that will foreseeably financially affect such interests.

If the disclosure provisions of the Act are applicable to any individual providing service under this Agreement, Contractor shall, upon execution of this Agreement, provide the County with the names, description of individual duties to be performed, and email addresses of all individuals, including but not limited to Contractor's employees, agents and subcontractors, who could be substantively involved in "mak[ing] a governmental decision" or "serv[ing] in a staff capacity" and in that capacity participating in making governmental decisions or performing duties that would be performed by an individual in a designated position, (2 CCR 18700.3), as part of Contractor's service to the County under this Agreement. Contractor shall immediately notify the County of the names and email addresses of any additional individuals later assigned to provide such service to the County under this Agreement in such a capacity. Contractor shall immediately notify the County of the names of individuals working in such a capacity who, during the course of the Agreement, end their service to the County. Contractor shall ensure that all such individuals identified pursuant to this paragraph understand that they are subject to the Act and shall conform to all requirements of the Act and other applicable conflict of interest and disclosure laws and regulations, and shall file Statements of Economic Interests within 30 days of commencing service pursuant to this Agreement, annually by April 1, and within 30 days of their termination of service pursuant to this Agreement.

If applicable, Contractor and its agents shall comply with California Government Code section 84308 ("Levine Act") and the applicable regulations of the Fair Political Practices Commission concerning campaign disclosure (2 California Code of Regulations sections 18438.1 – 18438.8), which (1) require a party to a proceeding involving a contract to disclose on the record of the proceeding any contribution, as defined by Government Code section 84308(a)(6), of more than $250 that the party or their agent has made within the prior 12 months, and (2) prohibit a party to a proceeding involving a contract from making a contribution, as defined by Government Code section 84308(a)(6), of more than $250 to any County officer during the proceeding and for 12 months following the final decision in the proceeding. Disclosures pursuant to the Levine Act must be submitted online at the Office of the Clerk of the Board of Supervisors website at http://www.sccgov.org/levineact.

9. Section 24, regarding Assignment, is hereby deleted and replaced with the following:

//

24. Assignment

The services performed by Contractor are personal in character. Contractor cannot assign, subcontract, or delegate any duties without the County's written consent. Any assignment, delegation, or subcontract by Contractor violating these restrictions is not enforceable against the County and confers no rights on any third party.

County agrees that Contractor may subcontract work under this Agreement to the following entities and persons: Michael Gennaco, Stephen Connolly, Julie Ruhlin, Teresa Magula, Margo Frasier, Dr. David Hellerstein, Kimberly Pearson, Karen Rea, Kevin Kuykendall, Howard Jordan, Kate Eves, Stacey Nelson, Flo Finkle, Brian Corr, and Samara Marion. In addition, County agrees that Contractor may subcontract with an individual to serve as its office administrator.

In the event that Contractor wishes to engage additional subcontractors who have expertise necessary to perform services required under this Agreement, Contractor shall identify the proposed subcontractors, their proposed scope of work, and their proposed hourly rates in the annual work plan, or an amendment thereto, presented to the Board for approval. Upon approval by the Board, Contractor may engage the subcontractors identified in its work plan to perform work under the Agreement.

Contractor shall be fully responsible for all work performed or required under this Agreement, including work performed by its subcontractors.

10. Section 25, regarding Notice, is hereby deleted and replaced with the following:

25. Notice

Except as otherwise stated, any notice required or permitted by this Agreement will be in writing and delivered as follows with notice deemed given as indicated: (a) by personal delivery when delivered personally; (b) by overnight courier upon written verification of delivery; (c) by telecopy or facsimile transmission upon acknowledgment of receipt of electronic transmission; or (d) by certified or registered mail, upon confirmation of delivery. The parties may deliver notice as follows:

To Contractor:

Julie Ruhlin
OIR Group
321 Loma Avenue
Long Beach, CA 90814
Phone: (562) 335-5443

To County:

Office of the Clerk of the Board of Supervisors
70 W. Hedding St., 10th Floor, East Wing
San José, CA 95110
Attn.: Clerk of the Board of Supervisors
Phone: (408) 299-5001
Facsimile: (408) 938-4525

With copy to:

Office of the County Counsel
70 W. Hedding. St., 9th Floor, East Wing
San José, CA 95110
Attn: Tony LoPresti, County Counsel

11. Section 31, regarding Survival, is hereby deleted and replaced with the following:

31. Survival

All representations, warranties, and covenants contained in this Agreement, or in any instrument, certificate, exhibit, or other writing intended by the parties to survive this Agreement, shall survive the termination or expiration of this Agreement, including but not limited to all terms (1) providing for indemnification of County; (2) relating to the California Public Records Act; (3) relating to County Data; and (4) relating to Contractor's obligations upon termination or expiration of this Agreement.

12. Section 32, regarding COVID-19 Requirements, is hereby added and incorporated into the Agreement as follows:

32. COVID-19 Requirements

Contractor shall comply with all County requirements in effect relating to COVID-19 for persons who routinely perform services for County onsite and share airspace with or proximity to other people at a County facility as part of their services for County as set forth in a County Health Order (or similar directives) available at https://covid19.sccgov.org/home, and incorporated herein by this reference. Contractor shall comply with all reasonable requests by County for documentation demonstrating Contractor's compliance with this Section.

13. Section 33, regarding ISO Security and Compliance Language, is hereby added and incorporated into the Agreement as follows:

Section 33. ISO Security and Compliance Language

(1) For purposes of this section, the following definitions shall apply:

(A) "Breach" means unauthorized access to, or use of, County Data or information security networks or systems that compromises confidentiality, integrity, and/or availability of those systems or County Data.

(B) "Independent Penetration Testing," or "pen testing," means the County's practice, by using an independent third party, of testing a

computer system, network or web application to find security vulnerabilities that an attacker could exploit.

(C) "Risk Assessment" means the process by which the County's Information Security Office ("ISO") assesses (i) the Contractor's information security program, and related aspects, by identifying, analyzing, and understanding how the Contractor will store, process and transmit County Data; and (ii) the potential impact on the County of any security risks, weaknesses and threats related to safeguarding County assets and County Data. The Risk Assessment usually includes the ISO's evaluation of documentation provided by the Contractor.

(2) Contractor shall do all of the following:

(A) Maintain or improve upon its information security posture at the time of the County's initial Risk Assessment as reasonably determined by the County. Contractor shall provide written notice to ISO of any changes or deficiencies to its information security posture.

(B) Protect the confidentiality, integrity, and availability of the County's data and comply with any information security requirements provided to Contractor by the ISO for the entire term of the Agreement.

(C) Follow any updated security requirements for the remaining term of the Agreement if the County re-evaluates the Risk Assessment, conducts periodic audits, and/or completes annual Independent Penetration Testing.

(D) Upon discovering any Breach that could impact the County, whether caused by Contractor, its officers, employees, contractors or agents or others, the Contractor shall notify the ISO at cybersecurityteam@iso.sccgov.org within 24 hours. Contractor shall also comply with all of its other obligations in this Agreement relating to breaches and potential breaches.

14. Section 34, regarding County Information Technology User Responsibility, is hereby added and incorporated into the Agreement as follows:

34. <u>County Information Technology User Responsibility</u>

Contractor shall comply with the County Information Technology User Responsibility Statement for Third Parties as set forth in Exhibit D, attached hereto and incorporated herein.

15. Section 35, regarding Remote Access, is hereby added and incorporated into the Agreement as follows:

35. Remote Access

Contractor shall comply with Exhibit E, regarding Remote Access, attached hereto and incorporated herein.

16. Section 36, regarding Living Wage, is hereby added and incorporated into the Agreement as follows:

36. Living Wage

Unless otherwise exempted or prohibited by law or County policy, where applicable, Contractors that contract with the County to provide Direct Services developed pursuant to a formal Request for Proposals process, as defined in County of Santa Clara Ordinance Code Division B36 ("Division B36") and Board Policy section 5.5.5.5 ("Living Wage Policy"), and their subcontractors, where the contract value is $100,000 or more ("Direct Services Contract"), must comply with Division B36 and the Living Wage Policy and compensate their employees in accordance with Division B36 and the Living Wage Policy. Compliance and compensation for purposes of this provision includes, but is not limited to, components relating to fair compensation, earned sick leave, paid jury duty, fair workweek, worker retention, fair chance hiring, targeted hiring, local hiring, protection from retaliation, and labor peace. If Contractor and/or a subcontractor violates this provision, the Board of Supervisors or its designee may, at its sole discretion, take responsive actions including, but not limited to, the following:

(a) Suspend, modify, or terminate the Direct Services Contract.

(b) Require the Contractor and/or Subcontractor to comply with an appropriate remediation plan developed by the County.

(c) Waive all or part of Division B36 or the Living Wage Policy.

This provision shall not be construed to limit an employee's rights to bring any legal action for violation of the employee's rights under Division B36 or any other applicable law. Further, this provision does not confer any rights upon any person or entity other than the Board of Supervisors or its designee to bring any action seeking the cancellation or suspension of a County contract. By entering into this contract, Contractor certifies that it is currently complying with Division B36 and the Living Wage Policy with respect to applicable contracts and warrants that it will continue to comply with Division B36 and the Living Wage Policy with respect to applicable contracts.

17. Exhibit B, Insurance Requirements for Professional Services Contracts, is hereby deleted and replaced with amended Exhibit B attached hereto.

18. Exhibit C, Business Associate Agreement, is hereby deleted and replaced with amended Exhibit C attached hereto.

Except as provided herein, all other provisions of the Agreement shall remain in full force and effect. In the event of a conflict between the Agreement and this amendment, the amendment shall control.

Each signatory warrants and represents that they executed this Agreement in their authorized capacity, and that they have the authority to bind the entity listed below to contractual obligations.

COUNTY OF SANTA CLARA

SUSAN ELLENBERG Date
President, Board of Supervisors

Signed and certified that a copy of this document has been delivered by electronic or other means to the President, Board of Supervisors.
ATTEST:

CURTIS BOONE
Acting Clerk of the Board of Supervisors

APPROVED AS TO FORM
AND LEGALITY:

DocuSigned by:
Laura Trice
7C70D23CD50B482...

LAURA S. TRICE
Deputy County Counsel

OIR Group, LLC

DocuSigned by:
Julie Ruhlin 1/3/2024
FC6869C33C6B44B...

Julie Ruhlin, Manager Date
OIR Group, LLC

INSURANCE REQUIREMENTS FOR PROFESSIONAL SERVICES CONTRACTS
(e.g. Medical, Legal, Financial services, etc.)

Indemnity

Notwithstanding any other provision of this Agreement, Contractor shall indemnify, release, hold harmless, and defend, with counsel approved by County of Santa Clara (hereinafter "County"), County and its officers, agents, and employees from any claim, demand, suit, judgment, liability, loss, injury, damage, or expense of any kind (including attorneys' fees and costs) arising out of, or in connection with, performance of this Agreement by Contractor and/or its officers, agents, employees, or sub-contractors, excepting only loss, injury, or damage caused by the sole negligence or willful misconduct of personnel employed by County. It is the intent of the parties to this Agreement to provide the broadest possible coverage for County as allowed by law. Contractor shall reimburse County for all costs, attorneys' fees, expenses, and liabilities incurred with respect to any litigation or process in which Contractor contests its obligation to indemnify, defend, and/or hold harmless County under this Agreement and does not prevail in that contest.

Insurance

Without limiting the Contractor's indemnification of the County, the Contractor shall provide and maintain at its own expense, during the term of this Agreement, or as may be further required herein, the following insurance coverages and provisions:

A. 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, a certified copy of the policy or policies shall be provided by the Contractor upon request.

This verification of coverage shall be sent to the requesting County department, unless otherwise directed. The Contractor shall not receive a Notice to Proceed with the work under the Agreement until it has obtained all insurance required and such insurance has been approved by the County. This approval of insurance shall neither relieve nor decrease the liability of the Contractor.

B. Qualifying Insurers

All coverages, 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- V, according to the current Best's Key Rating Guide or a company of equal financial stability that is approved by the County's Insurance Manager.

C. Notice of Cancellation

All coverage as required herein shall not be canceled or changed so as to no longer meet the specified County insurance requirements without 30 days' prior written notice of such cancellation or change being delivered to the County of Santa Clara or their designated agent.

D. Insurance Required

1. Commercial General Liability Insurance - for bodily injury (including death) and property damage which provides limits as follows:

   a. Each occurrence - $1,000,000

   b. General aggregate - $2,000,000

   c. Products/Completed Operations aggregate - $1,000,000

   d. Personal Injury - $1,000,000

2. General liability coverage shall include:

   a. Premises and Operations

   b. Personal Injury liability

   c. Products/Completed

   d. Severability of interest

3. General liability coverage shall include the following endorsement, a copy of which shall be provided to the County:

   Additional Insured Endorsement, which shall read:

   > "County of Santa Clara, and members of the Board of Supervisors of the County of Santa Clara, and the officers, agents, and employees of the County of Santa Clara, individually and collectively, as additional insureds."

   Insurance afforded by the additional insured endorsement shall apply as primary insurance, and other insurance maintained by the County of Santa Clara, its officers, agents, and employees shall be excess only and not contributing with insurance provided under this policy. Public Entities may also be added to the additional insured endorsement as applicable and the contractor shall be notified by the contracting department of these requirements.

4. Automobile Liability Insurance

For bodily injury (including death) and property damage which provides total limits of not less than one million dollars ($1,000,000) combined single limit per occurrence applicable to owned, non-owned and hired vehicles.

4a. Aircraft/Watercraft Liability Insurance (Required if Contractor or any of its agents or subcontractors will operate aircraft or watercraft in the scope of the Agreement)

For bodily injury (including death) and property damage which provides total limits of not less than one million dollars ($1,000,000) combined single limit per occurrence applicable to all owned non-owned and hired aircraft/watercraft.

5. Workers' Compensation and Employer's Liability Insurance

a. Statutory California Workers' Compensation coverage including broad form all-states coverage.

b. Employer's Liability coverage for not less than one million dollars ($1,000,000) per occurrence.

6. Professional Errors and Omissions Liability Insurance

a. Coverage shall be in an amount of not less than one million dollars ($1,000,000) per occurrence/aggregate.

b. If coverage contains a deductible or self-retention, it shall not be greater than fifty thousand dollars ($50,000) per occurrence/event.

c. Coverage as required herein shall be maintained for a minimum of two years following termination or completion of this Agreement.

7. Cyber Liability

a. Each occurrence - $1,000,000

b. General aggregate - $2,000,000

8. Cyber liability coverage shall include at a minimum, but not limited to:

a. Information Security and Privacy Liability

b. Privacy Notification Costs

9. Claims Made Coverage

If coverage is written on a claims made basis, the Certificate of Insurance shall clearly state so. In addition to coverage requirements above, such policy shall provide that:

a. Policy retroactive date coincides with or precedes the Contractor's start of work (including subsequent policies purchased as renewals or replacements).

b. Policy allows for reporting of circumstances or incidents that might give rise to future claims.

E. Special Provisions

The following provisions shall apply to this Agreement:

1. The foregoing requirements as to the types and limits of insurance coverage to be maintained by the Contractor and any approval of said insurance by the County or its insurance consultant(s) are not intended to and shall not in any manner limit or qualify the liabilities and obligations otherwise assumed by the Contractor pursuant to this Agreement, including but not limited to the provisions concerning indemnification.

2. The County acknowledges that some insurance requirements contained in this Agreement may be fulfilled by self-insurance on the part of the Contractor. However, this shall not in any way limit liabilities assumed by the Contractor under this Agreement. Any self-insurance shall be approved in writing by the County upon satisfactory evidence of financial capacity. Contractor’s obligation hereunder may be satisfied in whole or in part by adequately funded self-insurance programs or self-insurance retentions.

3. Should any of the work under this Agreement be sublet, the Contractor shall require each of its subcontractors of any tier to carry the aforementioned coverages, or Contractor may insure subcontractors under its own policies.

4. The County reserves the right to withhold payments to the Contractor in the event of material noncompliance with the insurance requirements outlined above.

F. Fidelity Bonds (Required only if contractor will be receiving advanced funds or payments)

Before receiving compensation under this Agreement, Contractor will furnish County with evidence that all officials, employees, and agents handling or having access to funds received or disbursed under this Agreement, or authorized to sign or countersign checks, are covered by a BLANKET FIDELITY BOND in an amount of AT LEAST fifteen percent (15%) of the maximum financial obligation of the County cited herein. If such bond is canceled or reduced, Contractor will notify County immediately, and County may withhold further payment to Contractor until proper coverage has been obtained. Failure to give such notice may be cause for termination of this Agreement, at the option of County.

EXHIBIT C

BUSINESS ASSOCIATE AGREEMENT

WHEREAS, the County of Santa Clara ("County") is a hybrid entity, performing both covered and non-covered functions under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and seeks to disclose certain Protected Health Information (defined below) to Contractor ("Business Associate") pursuant to the terms of the Agreement between the Parties to this Business Associate Agreement (BAA); and

WHEREAS, the County of Santa Clara Health System (CSCHS), which is part of the County and is comprised of multiple County Departments, including the Santa Clara Valley Medical Center Hospital and Clinics (SCVMC), O'Connor Hospital and Clinics (OCH), St. Louise Regional Hospital and Clinics (SLRH), the Behavioral Health Services Department (BHSD), the County Public Health Department (PHD), the County Custody Health Services Department (CHSD), and the Valley Health Plan (VHP); and

WHEREAS, CSCHS and the additional County departments and offices designated in the County of Santa Clara Board of Supervisors Policy Manual Section 3.40 (General Policy Relating to the Health Insurance Portability and Accountability Act of 1996 (HIPAA)) (HIPAA) are a "covered entity" under HIPAA and shall be referred to as the "Covered Entity" for purposes of this BAA; and

WHEREAS, the Covered Entity and Business Associate intend to protect the privacy and provide for the security of PHI used and disclosed pursuant to this BAA in compliance with HIPAA; the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 (the "HITECH Act"), and regulations promulgated thereunder by the U.S. Department of Health and Human Services (collectively, the "HIPAA Regulations"); California Welfare & Institutions Code Section 5328; 42 U.S.C. Section 290dd-2; 42 C.F.R Part 2; California Confidentiality of Medical Information Act (Civil Code, §56 *et seq.*); California Health & Safety Code Section 1280.15 *et seq.*; and other applicable laws; and to the extent the Business Associate is to carry out the Covered Entity's obligation under the Privacy Rule (defined below), the Business Associate must comply with the requirements of the Privacy Rule that apply to the Covered Entity in the performance of such obligation.

WHEREAS, part of the HIPAA Regulations, the Privacy Rule and the Security Rule (both of which are defined below) require covered entities to enter into a contract containing specific requirements with any business associate prior to the disclosure of PHI, as set forth in, but not limited to, Title 45, Sections 164.314(a), 164.502(e), and 164.504(e) of the Code of Federal Regulations (C.F.R.) and contained in this BAA.

NOW, THEREFORE, in consideration of the mutual promises below and the exchange of information pursuant to the BAA, the Parties agree as follows:

I. Definitions

Terms used, but not otherwise defined, and terms with initial capital letters in the BAA have the same meaning as defined under HIPAA, the HITECH Act, HIPAA Regulations, and other applicable laws.

Business Associate is a person, organization, or agency other than a workforce member that provides specific functions, activities, or services that involve the use, creation, or disclosure of PHI for, or on behalf of, a HIPAA covered health care component. Examples of business associate functions are activities such as claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, practice management, repricing; and legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.

Designated Record Set shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. §164.501.

Electronic Protected Health Information or ePHI means Protected Health Information that is maintained in or transmitted by electronic media as defined by 45 C.F.R. § 160.103.

Electronic Health Record shall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C. Section 17921.

Health Care Operations shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. §164.501.

Privacy Breach shall mean any acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted or allowed under state or federal privacy laws.

Privacy Rule shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and E.

Protected Health Information or PHI means any information, whether oral or recorded in any form or medium: (i) that relates to the past, present, or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under the Privacy Rule, including, but not limited to, 45 C.F.R. §160.103. Protected Health Information includes ePHI.

Protected Information shall mean PHI provided by Covered Entity to Business Associate or created or received by Business Associate on the Covered Entity's behalf.

Security Incident shall mean, as set forth in 45 C.F.R. § 164.304, "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system." Security Incident shall not include, (a) unsuccessful attempts to penetrate computer networks or servers maintained by Business

Associate, or (b) immaterial incidents that occur on a routine basis, such as general "pinging" or "denial of service" attacks.

Security Rule shall mean the HIPAA Regulation that is codified at 45 C.F.R. Parts 160 and 164, Subparts A and C.

Unsecured PHI shall have the meaning given to such term under the HITECH Act and any guidance issued pursuant to such Act including, but not limited to, 42 U.S.C. Section 17932(h)(1) and 45 C.F.R. § 164.402.

II. Duties & Responsibilities of Business Associate

a. Permitted and Prohibited Uses. Business Associate shall use Protected Information only for the purpose of performing Business Associate's obligations under the Agreement, as otherwise permitted or required under the Agreement, and for:

(i) the proper management and administration of Business Associate, (ii) to carry out the legal responsibilities of Business Associate, or (iii) data aggregation purposes for the Health Care Operations of Covered Entity. [45 C.F.R. §§ 164.502(a)(3), 164.504(e)(2)(ii)(A) and 164.504(e)(4)(i)]. Further, Business Associate shall not use Protected Information in any manner that would constitute a violation of the Privacy Rule, Welfare & Institutions Code Section 5328, 42 C.F.R. Part 2, the HITECH Act, or other applicable law if so used by Covered Entity.

b. Permitted and Prohibited Disclosures. Business Associate shall not disclose Protected Information except for the purpose of performing Business Associate's obligations under the Agreement, as permitted or required under the Agreement, and as required by law. Business Associate shall not disclose Protected Information in any manner that would constitute a violation of the Privacy Rule, 42 C.F.R. Part 2, Welfare & Institutions Code Section 5328, the HITECH Act, or other applicable law if so disclosed by Covered Entity. However, Business Associate may disclose Protected Information (i) for the proper management and administration of Business Associate; (ii) to carry out the legal responsibilities of Business Associate; or (iii) for data aggregation purposes for the Health Care Operations of Covered Entity. If Business Associate discloses Protected Information to a third party, Business Associate must obtain, prior to making any such disclosure, (i) reasonable written assurances from such third party that such Protected Information will be held confidential as provided pursuant to this BAA and only disclosed as required by law or for the purposes for which it was disclosed to such third party, and (ii) a written agreement from such third party to immediately notify Business Associate of any Privacy Breaches of confidentiality of the Protected Information within twenty-four (24) hours of discovery, to the extent it has obtained knowledge of such Privacy Breach. [42 U.S.C. §17932; 45 C.F.R. §§ 164.504(e)(2)(i)-(ii)(A) and 164.504(e)(4)(ii)].

c. Additional Prohibited Uses and Disclosures. Business Associate shall not use or disclose Protected Information for fundraising or marketing purposes. [42 U.S.C. §17936(a) and 45 C.F.R. § 164.501]. Business Associate shall not disclose Protected Information to a health plan for payment or health care operations purposes if the individual has requested this special restriction, and has paid out of pocket in full for the health care item or service to which the Protected Information solely relates. [42 U.S.C. §17935(a); 45 C.F.R. §164.502(a)(5)(ii)]. Business

Associate shall not directly or indirectly receive remuneration in exchange for Protected Information, except with the prior written consent of Covered Entity and as permitted by the HITECH Act. [42 U.S.C. §17935(d)(2)]. This prohibition shall not affect payment by Covered Entity to Business Associate for services provided pursuant to the Agreement.

d. Appropriate Safeguards. Business Associate shall implement appropriate administrative, technological, and physical safeguards as are necessary to prevent the use or disclosure of Protected Information other than as permitted by this BAA that reasonably and appropriately protect the confidentiality, integrity, and availability of the Protected Information, and comply, where applicable, with the HIPAA Security Rule with respect to Electronic PHI. Business Associate, including any of its agents and subcontractors, shall not create, receive, maintain, transmit, or store Protected Information outside the United States.

e. Reporting of Improper Access, Use, or Disclosure. Business Associate shall notify Covered Entity via the CSCHS Ethics, Privacy & Compliance Office (as detailed below) within twenty–four (24) hours of any suspected or actual Privacy Breach of Protected Information; any use or disclosure of Protected Information not permitted by this Agreement; any security incident (*i.e.*, any attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in any information system) related to Protected Information, and any actual or suspected use or disclosure of data in violation of any applicable federal or state laws by Business Associate or its agents or subcontractors.

Business Associate shall report to CSCHS Ethics, Privacy & Compliance Office in writing any suspected or actual access, use, or disclosure of Protected Information not permitted by the Agreement, including this BAA, and any other applicable state or federal law, including, but not limited to 42 U.S.C. Section 17921; 45 C.F.R. §164.504(e)(2) (ii) (C); 45 C.F.R. §164.308(b); California Health & Safety Code Section 1280.15, California Confidentiality of Medical Information Act (California Civil Code Section 56.10), California Welfare & Institutions Section 5328 to the following contacts:

Ethics, Privacy & Compliance Office
County of Santa Clara Health System
2325 Enborg Lane, Suite 290
San Jose, California 95128
Facsimile: (408) 885-6006 Telephone: (408) 885-3794
Email: ComplianceOfficer@hhs.sccgov.org

Notification shall include, to the extent possible, the following: (1) a brief description of what happened, including the date of the suspected or actual Privacy Breach and/or Security Incident, and the date of the discovery of the Privacy Breach, if known and applicable; (2) the location of the breached information; (3) the unauthorized person who used the Protected Information or to whom the disclosure was made; (4) whether the Protected Information was actually acquired or viewed; (5) a description of the types of Protected Information that were involved in the Privacy Breach and/or Security Incident; (6) safeguards in place prior to the Privacy Breach and/or Security Incident; (7) actions taken in response to the Privacy Breach and/or Security Incident; (8) any steps individuals should take to protect themselves from potential harm resulting from the Privacy Breach and/or Security Incident; (9) a brief description of what the business

associate is doing to investigate the Privacy Breach and/or Security Incident, to mitigate harm to individuals, and to protect against further Privacy Breaches and/or Security Incidents; and (10) contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, and website or postal address. [45 C.F.R. §§164.410(c) and 164.404(c)]. Business Associate shall take any action pertaining to such actual or suspected Privacy Breach and/or Security Incident required by applicable federal and state laws and regulations, including 45 C.F.R. §164.410 with respect to reporting Privacy Breaches of Unsecured PHI. [42 U.S.C. §17921; 45 C.F.R. §§164.504(e)(2)(ii)(C), Section 164.308(b)]

f. Business Associate's Agents and Subcontractors. Business Associate shall ensure that any agents or subcontractors to whom it provides Protected Information agree in writing to the same restrictions and conditions that apply to Business Associate with respect to such Protected Information and implement the safeguards required by paragraph (II)(d) above with respect to Electronic PHI provided by Covered Entity or created or received on Covered Entity's behalf. [45 C.F.R. §§ 164.502(e)(1)(ii), 164.504(e)(2)(ii)(D) and 164.308(b)]. If Business Associate knows of a pattern of activity or practice of an agent or subcontractor that constitutes a material breach or violation of an agent or subcontractor's obligations under their contract or addendum or other arrangement with the agent or subcontractor, the Business Associate must take reasonable steps to cure the breach or end the violation. If these steps are unsuccessful, Business Associate shall sanction or terminate the contract or arrangement with agent or subcontractor, if feasible. [45 C.F.R. §164.504(e)(1)(iii)]. Business Associate shall provide written notification to Covered Entity of any pattern of activity or practice of a subcontractor or agent that Business Associate believes constitutes a material breach or violation of the agent or subcontractor's obligations under the contract or addendum or other arrangement with the agent or subcontractor within twenty four (24) hours of discovery and shall meet with Covered Entity to discuss and attempt to resolve the problem as one of the reasonable steps to cure the breach or end the violation.

g. Access to Protected Information. Business Associate shall make Protected Information maintained by Business Associate or its agents or subcontractors in Designated Record Sets available to Covered Entity for inspection and copying within ten (10) days of a request by Covered Entity to enable Covered Entity to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. §164.524. [45 CF.R. Section 164.504(e)(2)(ii) (E); 42 C.F.R. part 2 and Welfare & Institutions Code Section 5328]. If Business Associate maintains an Electronic Health Record, Business Associate shall provide such information in electronic format to enable Covered Entity to fulfill its obligations under the HITECH Act, including, but not limited to, 42 U.S.C. Section 17935(e)(1). If any individual requests access to Protected Information Covered Entity in writing within five (5) days of the request.

h. Electronic PHI. If Business Associate receives, creates, transmits, or maintains ePHI on behalf of Covered Entity, Business Associate will, in addition, do the following:

(1) Develop, implement, maintain, and use appropriate administrative, physical, and technical safeguards in compliance with Section 1173(d) of the Social Security Act, Title 42, Section 1320(s) or the United States Code and Title 45, Part 162 and 164 of C.F.R. to preserve the integrity and confidentiality of all ePHI received from or on behalf of Covered Entity.

(2) Document and keep these security measures current and available for inspection by Covered Entity.
(3) Ensure that any agent, including a subcontractor, to whom the Business Associate provides ePHI received from or on behalf of Covered Entity, agrees to implement reasonable and appropriate safeguards to protect it.
(4) Report to the Covered Entity, as provided in Section 2(d), any actual or suspected Privacy breach and/or Security Incident of which it becomes aware.

i. Amendment of Protected Information. Within ten (10) days of receipt of a request from Covered Entity for an amendment of Protected Information or a record about an individual contained in a Designated Record Set, Business Associate or its agents or subcontractors shall make such Protected Information available to Covered Entity for amendment and incorporate any such amendment to enable Covered Entity to fulfill its obligations under the Privacy Rule. If any individual requests an amendment of Protected Information directly from Business Associate or its agents or subcontractors, Business Associate must notify Covered Entity in writing within five (5) days of the request. Any approval or denial of amendment of Protected Information maintained by Business Associate or its agents or subcontractors shall be the responsibility of Covered Entity.

j. Accounting Rights. Business Associate agrees to document such disclosures of Protected Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an individual for an accounting of disclosures of PHI in accordance with the Privacy Rule and the HITECH Act. [42 U.S.C. § 17935(c) and 45 C.F.R. § 164.528]. Business Associate agrees to implement a process that allows for an accounting of disclosures to be collected and maintained by Business Associate and its agents or subcontractors for at least six (6) years prior to the request. Accounting of disclosures from an Electronic Health Record for treatment, payment or health care operations purposes are required to be collected and maintained for three (3) years prior to the request, and only to the extent Business Associate maintains an Electronic Health Record and is subject to this requirement.

At a minimum, the information collected and maintained shall include: (i) the date of disclosure; (ii) the name of the entity or person who received Protected Information and, if known, the address of the entity or person; (iii) a brief description of Protected Information disclosed and (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the individual's authorization, or a copy of the written request for disclosure. [45 C.F.R. §164.528(b)]. In the event that the request for an accounting is delivered directly to Business Associate or its agents or subcontractors, Business Associate shall forward it to Covered Entity in writing within five (5) days of the request. It shall be Covered Entity's responsibility to prepare and deliver any such accounting requested. Business Associate shall not disclose any Protected Information except as set forth in the Agreement and this BAA.

k. Governmental Access to Records. Business Associate shall make its internal practices, books, and records relating to the use and disclosure of Protected Information available to Covered Entity and to the Secretary of the U.S. Department of Health and Human Services (the "Secretary") for purposes of determining Business Associate's compliance with the Privacy Rule). [45 C.F.R. §164.504(e)(2)(ii)(I)]. Business Associate shall concurrently provide to Covered Entity

a copy of any internal practices, books, and records relating the use and disclosure of Protected Information that Business Associate provides to the Secretary.

l. Minimum Necessary. Business Associate and its agents or subcontractors shall request, use, and disclose only the minimum amount of Protected Information reasonably necessary to accomplish the purpose of the request, use, or disclosure in accordance with 42 U.S.C. Section 17935(b).

m. Protected Information Ownership. Business Associate acknowledges that Business Associate has no ownership rights with respect to the Protected Information governed by this BAA, and all rights, interests, and title remain vested in the County at all times.

n. Warranties and Disclosures. Business Associate assumes risk for any and all use of Protected Information. Covered Entity assumes no liability or responsibility for any errors or omissions in, or reliance upon, the Protected Information, including, but not limited to information electronic systems. Covered Entity makes no representations or warranties of any kind, express or implied, including but not limited to: accuracy, completeness, or availability of content, non-infringement, merchantability, or fitness for a particular use or purpose. Covered Entity does not warrant that Protected Information is free of viruses or other harmful components or that service will be uninterrupted or error-free, or that defects will be corrected.

o. Audits, Inspection, and Enforcement. Within ten (10) days of a written request by Covered Entity, Business Associate and its agents or subcontractors shall allow Covered Entity to conduct a reasonable inspection of the facilities, systems, books, records, agreements, policies, and procedures relating to the use or disclosure of Protected Information pursuant to this BAA for the purpose of determining whether Business Associate has complied with this BAA; provided, however, that (i) Business Associate and Covered Entity shall mutually agree in advance upon the scope, timing, and location of such an inspection; (ii) Covered Entity shall protect the confidentiality of all confidential and proprietary information of Business Associate to which Covered Entity has access during the course of such inspection; and (iii) Covered Entity shall execute a nondisclosure agreement, upon terms mutually agreed upon by the parties, if requested by Business Associate.

The fact that Covered Entity inspects, or fails to inspect, or has the right to inspect, Business Associate's facilities, systems, books, records, agreements, policies, and procedures does not relieve Business Associate of its responsibility to comply with the BAA, nor does Covered Entity's (i) failure to detect any unsatisfactory practices; or (ii) detection, but failure to notify Business Associate or require Business Associate's remediation of any unsatisfactory practices; constitute acceptance of such practice or a waiver of Covered Entity's enforcement rights under the Agreement or BAA. Business Associate shall notify Covered Entity within five (5) days of learning that Business Associate has become the subject of an audit, compliance review, or complaint investigation by the Office for Civil Rights of the U.S. Department of Health and Human Services.

III. Termination

a. Material Breach. A Breach by Business Associate of any provision of this BAA shall constitute a material breach of the Agreement and shall provide grounds for immediate

termination of the Agreement, notwithstanding any provision in the Agreement to the contrary. [45 C.F.R. §164.504(e)(2)(iii)].

b. Judicial or Administrative Proceedings. Covered Entity may terminate the Agreement, effective immediately, if (i) Business Associate is named as a defendant in a criminal proceeding for a violation of HIPAA, the HITECH Act, 42 C.F.R. Part 2, the HIPAA Regulations or other security or privacy laws; or (ii) a finding or stipulation that the Business Associate has violated any standard or requirement of HIPAA, the HITECH Act, 42 C.F.R. Part 2, the HIPAA Regulations or other security or privacy laws is made in any administrative or civil proceeding.

c. Effect of Termination. Upon termination of the Agreement for any reason, Business Associate shall, at the option of Covered Entity, immediately return or destroy all Protected Information that Business Associate or its agents or subcontractors still maintain in any form, and shall retain no copies of such Protected Information. If return or destruction is not feasible, Business Associate shall continue to extend the protections of Section II of the BAA to such information, and limit further use of such Protected Information to those purposes that make the return or destruction of such Protected Information infeasible. [45 C.F.R. § 164.504(e)(ii)(2)(I)]. If County elects destruction of the Protected Information, Business Associate shall certify in writing to County that such Protected Information has been destroyed.

IV. General Provisions

a. Indemnification. In addition to the indemnification language in the Agreement, Business Associate agrees (i) to be responsible for, and defend, indemnify, and hold harmless the Covered Entity for any breach of Business Associate's privacy or security obligations under the Agreement, including any fines, penalties, and assessments that may be made against Covered Entity or the Business Associate for any Privacy Breaches or late reporting; and (ii) to pay and bear responsibility for the cost of and notice for any credit monitoring services.

b. Disclaimer. Covered Entity makes no warranty or representation that compliance by Business Associate with this BAA, HIPAA, the HITECH Act, or the HIPAA Regulations will be adequate or satisfactory for Business Associate's own purposes. Business Associate is solely responsible for all decisions made by Business Associate regarding the use and safeguarding of PHI.

c. Amendment to Comply with Law. The parties acknowledge that state and federal laws relating to data security and privacy are evolving and that amendment of the Agreement or BAA may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule and other applicable California laws relating to the security or confidentiality of PHI. Upon the request of any Party, the other Party agrees to promptly enter into negotiations concerning the terms of an amendment to the BAA embodying written assurances consistent with the standards and requirements of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule and other applicable California laws relating to the security or confidentiality of PHI.

Covered Entity may terminate the Agreement between the Parties or the provisions of this BAA upon thirty (30) days written notice in the event (i) Business Associate does not promptly

enter into negotiations to amend the Agreement when requested by Covered Entity pursuant to this section or (ii) Business Associate does not enter into an amendment to the Agreement providing assurances regarding the safeguarding of Protected Information that Covered Entity, in its sole discretion, deems sufficient to satisfy the standards and requirements of applicable laws.

d. Assistance in Litigation of Administrative Proceedings. Business Associate shall notify Covered Entity within forty-eight (48) hours of any litigation or administrative proceedings commenced against Business Associate or its agents or subcontractors. Business Associate shall make itself, and any subcontractors, employees, or agents assisting Business Associate in the performance of its obligations under the Agreement, including this BAA, available to Covered Entity, at no cost to Covered Entity, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against Covered Entity, officers or employees based upon a claimed violation of HIPAA, the HITECH Act, the Privacy Rule, the Security Rule, or other laws relating to security and privacy, except where Business Associate or its subcontractor, employee, or agent is named as an adverse party.

e. No Third-Party Beneficiaries. Nothing express or implied in the Agreement, including this BAA, is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Business Associate, and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

f. Effect on Agreement. Except as specifically required to implement the purposes of the BAA, or to the extent inconsistent with this BAA, all other terms of the Agreement shall remain in force and effect.

g. Interpretation. The BAA shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HITECH Act, the Privacy Rule, and the Security Rule. The parties agree that any ambiguity in this BAA shall be resolved in favor of a meaning that complies and is consistent with HIPAA, the HITECH Act, 42 C.F.R. Part 2, the Privacy Rule, and the Security Rule and other applicable California laws relating to the security or confidentiality of PHI.

h. Governing Law, Venue. This Business Associate Agreement has been executed and delivered in, and shall be construed and enforced in accordance with, the laws of the State of California. Proper venue for legal action regarding this Agreement shall be in the County of Santa Clara.

i. Survivorship. The respective rights and responsibilities of Business Associate related to the handling of Protected Information survive termination of this Agreement.

V. Drug and Alcohol Records

a. Covered Entity and Business Associate agree that when drug and alcohol treatment records are included in the contracted scope of services, the Business Associate will act as a "qualified service organization" or a "QSO" within the meaning of the federal law governing Confidentiality of Alcohol and Drug Abuse Patient Records and its implementing regulations, 42 C.F.R. Part 2; and

b. Adherence to the Requirements of 42 C.F.R. Business Associate acknowledges that in receiving, transmitting, transporting, storing, processing, or otherwise dealing with records

and information for CSCHS patients under this Agreement and BAA, it is fully bound by the regulations governing confidentiality of alcohol and drug abuse patient records, 42 C.F.R. §2.1 *et seq*., and HIPAA, and may not use or disclose the information except as permitted or required by this BAA or applicable law.

c. Resist Efforts in Judicial Procedures. Business Associate agrees to resist any efforts in judicial proceedings to obtain access to the Protected Information except as expressly provided for in the regulations governing the Confidentiality of Alcohol and Drug Abuse Records, 42 C.F.R. Part 2.

EXHIBIT D

COUNTY INFORMATION TECHNOLOGY USER RESPONSIBILITY STATEMENT FOR THIRD PARTIES

1. DEFINITIONS

(a) *"County Confidential Information"* is all material non-public information, written or oral, disclosed, directly or indirectly, through any means of communication or observation by County to Contractor or any of its affiliates or representatives

(b) *"County Systems"* include but are not limited to, all County-owned, leased or managed servers, mainframe computers, desktop computers, laptop computers, handheld devices (including smart phones, wireless PDAs and Pocket PCs), equipment, networks, application systems, databases, software, phone systems, any device with network capabilities (e.g., a workstation with an attached modem, routers, switches, laptop computers, handheld devices), and any other system that stores, processes, and/or transmits County-owned information/data. These items are typically under the direct control and management of the County. "County Systems" also include these items when they are under the control and management of a service provider for use by County, as well as any personally-owned device that an individual has express written permission to use for County purposes.

(c) "County-owned information/data," for purposes of this Exhibit is any information or data that is transported across a County network, or that resides in a County-owned information system, or on a network or system under the control and management of a service provider for use by County. This information/data is the exclusive property of County unless constitutional provision, State or Federal statute or case law provide otherwise. County-owned information/data does not include a User's personal, non-County business information, communications, data, files and/or software transmitted by or stored on a personally-owned device if that information/data is not transported across a County network or does not reside in a County System or on a network or system under the control and management of a service provider for use by County.

(d) *"Mobile Device"* is any portable computing device that fits one of the following categories: laptops, smartphones, or tablets. "Mobile Device" does not include devices that are used exclusively for the purpose of making telephone calls.

(e) *"Users"* include all employees, agents and/or representatives of Contractor performing services under this Agreement.

2. GENERAL REQUIREMENTS

(a) Contractor will provide Users with a written copy of this Exhibit and will ensure that Users know, understand and comply with the requirements of this Exhibit. Users allowed access to County resources shall sign the Acknowledgement and Receipt. In all cases, such access shall be subject to approval by an authorized County representative.

(b) Users are personally responsible for knowing and understanding these requirements, and are personally responsible for any actions they take that do not comply with County policies and standards. If a User is unclear as to requirements, User shall ask County for guidance.

(c) If a User is issued an account for a County System, User shall comply with the following County standards for password definition, use, and management:

(i) Minimum password length is 12 characters unless a particular County System has a different requirement or is not technically feasible.
(ii) The password must be high complexity (contains one of each, upper, lower, number, symbol).
(iii) The password must be rotated every 90 days.
(iv) User must not reuse the last 10 passwords.
(v) Access to County System is denied after 5 failed logon attempts.

(d) Only authorized County staff may attach any form of computer equipment to a County network or system. This includes, but is not limited to, attachment of such devices as mobile devices, peripherals (e.g., external hard drives, printers), and USB storage media. It excludes County wireless networks provided specifically for the use of guests or visitors to County facilities.

(e) User shall not use USB storage media on any County System. All such devices shall be County-owned, formally issued to User by County, and used only for legitimate County purposes.

(f) User shall not connect County-owned computing equipment, including USB storage media, to non-County systems or networks, unless County gives its express written permission. This formal approval process ensures that the non-County system or network in question has been evaluated for compliance with County security standards. An example of a permitted connection to a non-County system or network would be approved connection of a County issued laptop to a home network.

(g) User shall not install, configure, or use any device intended to provide connectivity to a non-County network or system (such as the Internet), on any County System, without County's express written permission. If authorized to install, configure or use such a device, User shall comply with all applicable County standards designed to ensure the privacy and protection of data, and the safety and security of County Systems. Any allowed installation shall not be activated until it is reviewed and approved in writing by an authorized County representative.

(h) The unauthorized implementation or configuration of encryption, special passwords, biometric technologies, or any other methods to prevent access to County resources by those individuals who would otherwise be legitimately authorized to do so is prohibited.

(i) Users shall not attempt to elevate or enhance their assigned level of privileges unless County gives its express written permission. Users who have been granted enhanced

privileges due to their specific roles, such as system or network administrators, shall not abuse these privileges and shall use such privileges only in the performance of appropriate, services performed under this Agreement.

(j) Users shall use County-approved authentication mechanisms when accessing County networks and systems, and shall not deactivate, disable, disrupt, or bypass (or *attempt* to deactivate, disable, disrupt, or bypass) any security measure or security configuration implemented by County.

(k) Users shall not circumvent, or attempt to circumvent, legal guidelines on software use and licensing. If a User is unclear as to whether a software program may be legitimately copied or installed, it is the responsibility of the User to check with County.

(l) All software on County Systems shall be installed by authorized County support staff except as provided in this Agreement. Users may not download or install software on any County system unless express written permission has been obtained from County such as in this Agreement.

(m) Users shall immediately report to the County TechLink Center the loss or theft of County-owned computer equipment, or of personally-owned computer equipment that has been approved for use in conducting County business or performing services under a Supplemental Agreement. The County Service Desk contact information is (408) 970-2222 or support@tss.sccgov.org.

(n) Users must be aware of security issues and shall immediately report incidents to the County Information Security Office involving breaches of the security of County Systems or breaches of County-owned information/data, such as the installation of an unauthorized device, or a suspected software virus or other occurrences of malicious software or content. The Information Security Office's contact information is cybersecurityteam@iso.sccgov.org.

(o) Users shall respect the sensitivity, privacy and confidentiality aspects of all County-owned information. In particular:

(i) Users shall not access, or attempt to access, County Systems or County-owned information/data unless specifically authorized to do so by the terms of this Agreement.

(ii) If User is assigned a County account, User shall not allow unauthorized individuals to use their account; this includes the sharing of account passwords.

(iii) Users shall not without County's written permission, use or disclose County-owned information/data other than in the performance of its obligations under this Agreement.

(iv) Users shall take every precaution to ensure that all confidential or restricted information is protected from disclosure to unauthorized individuals.

(v) Users shall not make or store paper or electronic copies of information unless required to provide services under this Agreement.

(vi) Users shall comply with all confidentiality requirements in Contractor's Agreement with the County. Users shall not use or disclose County Confidential Information other than in the performance of its obligations for County. All County Confidential Information shall remain the property of the County. User shall not acquire any ownership interest in County Confidential Information.

(p) Users shall do all of the following:

(i) Users shall not change or delete County-owned information/data unless performing such changes is required to perform services under this Agreement.

(ii) Users shall avoid actions that might introduce malicious software, such as viruses or worms, onto any County system or network.

(iii) Upon termination or expiration of this Agreement, Users shall not retain, give away, or remove any County-owned information/data or document from any County System or County premises. Users shall return to County all County-owned assets, including hardware and data.

(q) Electronic information transported across any County network, or residing in any County System, is potentially subject to access by County technical support staff, other County personnel, and the general public. Users should not presume any level of privacy for data transmitted over a County network or stored on a County System.

(r) Users must protect, respect and not infringe upon all intellectual property rights, including but not limited to rights associated with patents, copyrights, trademarks, trade secrets, proprietary information, County Confidential Information, and confidential information belonging to any other third party.

(s) All information resources on any County System are the property of County and are therefore subject to County policies regarding acceptable use. No User may use any County System or County-owned information/data for the following purposes:

(i) Personal profit, including commercial solicitation or conducting or pursuing their own business interests or those of another organization that are not related to the User conducting County business. This prohibition does not apply to User's performance of contractual obligations for the County.

(ii) Unlawful or illegal activities, including downloading licensed material without authorization, or downloading copyrighted material from the Internet without the publisher's permission.

(iii) To access, create, transmit, print, download or solicit material that is, or may be construed to be, harassing or demeaning toward any individual or group for any reason, including but not limited to on the basis of sex, age, race, color, national

origin, creed, disability, political beliefs, organizational affiliation, or sexual orientation, unless doing so is legally permissible and necessary in the course of conducting County business.

(iv) To access, create, transmit, print, download or solicit sexually-oriented messages or images, or other potentially offensive materials such as, but not limited to, violence, unless doing so is legally permissible and necessary in the course of conducting County business.

(v) Knowingly propagating or downloading viruses or other malicious software.

(vi) Disseminating hoaxes, chain letters, or advertisements.

3. INTERNET AND EMAIL

(a) Users shall not use County Systems for personal activities.

(b) When conducting County business or performing services under this Agreement, Users shall not configure, access, use, or participate in any Internet-based communication or data exchange service unless express written permission has been given by County. Such services include, but are not limited to, file sharing (such as Dropbox, Box, Google OneDrive), Instant Messaging (such as AOL IM), email services (such as Hotmail and Gmail), peer-to-peer networking services (such as Kazaa), and social networking services (such as blogs, Instagram, Snapchat, MySpace, Facebook and Twitter). If a User has received express written permission to access such services, User shall comply with all relevant County policies, procedures, and guidelines.

(c) Users assigned a County email account must comply with the County's Records Retention and Destruction Policy.

(d) Users shall not use an internal County email account assigned to another individual to either send or receive email messages.

(e) Users shall not configure a County email account so that it automatically forwards messages to an external Internet email system unless County gives its express written permission.

4. REMOTE ACCESS

(a) Users are not permitted to implement, configure, or use any remote access mechanism unless the County has authorized the remote access mechanism.

(b) County may monitor and/or record remote access sessions, and complete information on the session logged and archived. Users have no right, or expectation, of privacy when remotely accessing County Systems or County-owned information/data. County may use audit tools to create detailed records of all remote access attempts and remote access sessions, including User identifier, date, and time of each access attempt.

(c) User shall configure all computer devices used to access County resources from a remote location according to NIST 800-53 standards, or an equivalent industry standard. These include approved, installed, active, and current: anti-virus software, software or hardware-based firewall, full hard drive encryption, and any other security software or security-related system configurations that are required and approved by County.

(d) Users that have been provided with a County-owned device intended for remote access use, such as a laptop or other Mobile Device, shall ensure that the device is protected from damage, access by third parties, loss, or theft. Users shall immediately report loss or theft of such devices to the County Service Desk: (408) 970-2222 or support@tss.sccgov.org.

(e) Users shall protect the integrity of County Systems and County-owned information/data while remotely accessing County resources, and shall immediately report any suspected security incident or concern to the County Information Security Office at cybersecurityteam@iso.sccgov.org.

(f) Users shall comply with any additional remote access requirements in this Agreement such as an Exhibit on Remote Access.

5. THIRD PARTY-OWNED DEVICES

(a) This Section 5 applies if County permits Users to perform services under this Agreement with devices not owned by the County ("Third-party owned device"). Third-party owned devices include devices with email and/or data storage capability (such as laptops, iPhones, iPads, Android phones and tablets, BlackBerry and other "smart" devices).

(b) The third party-owned device in question shall use existing, County-approved and County-owned access/authentication systems when accessing County Systems.

(c) Users shall allow County to configure third party-owned devices as appropriate to meet security requirements, including the installation of specific security software mandated by County policy.

(d) Use of a third party-owned device shall comply with County policies and procedures for ensuring that software updates and patches are applied to the device according to a regular, periodic schedule on at least a monthly basis. County may verify software installations and updates.

(e) Users have no expectation of privacy with respect to any County-owned communications, information, or files on any third party-owned device. User agrees that, upon request, the County may immediately access any and all work-related or County-owned information/ data stored on these devices, in order to ensure compliance with County policies.

(f) Users shall adhere to all relevant County security policies and standards, just as if the third party-owned device were County property. This includes, but is not limited to,

policies regarding password construction and management, physical security of the device, device configuration including full storage encryption, and hard drive and/or storage sanitization prior to disposal.

(g) Users shall not make modifications of any kind to operating system configurations implemented by County on the device for security purposes, or to any hardware or software installed on the device by County.

(h) Users shall treat the contract-related or County-owned communications, information or files the third-party owned device contains as County property. User shall not allow access to or use of any work-related or County-owned communications, information, or files by individuals who have not been authorized by County to access or use that data.

(i) Users shall report immediately to the County Information Security Office cybersecurityteam@iso.sccgov.org, any incident or suspected incident of unauthorized access and/or disclosure of County resources, data, or networks that involve the third-party owned device, and shall report the loss or theft of the device immediately to the County Service Desk: (408) 970-2222 or support@tss.sccgov.org.

6. ACKNOWLEDGEMENT AND RECEIPT

This Acknowledgement hereby incorporates the URS.

By signing below, I acknowledge that I have read and understand all sections of this URS. I also acknowledge that violation of any of its provisions may result in disciplinary action, up to and including termination of my relationship with County and/or criminal prosecution.

Have you been granted Remote Access ☐ Yes ☐ No

I have read and understand the contents of the URS regarding Remote Access and the Exhibit on Remote Access. I understand that violation of these provisions may result in disciplinary action, up to and including termination of my relationship with the County and/or criminal prosecution. I received approval from County for remote access for legitimate County business, as evidenced by the signatures below.

User Signature: Date Signed:

_____

Print User Name:

_____

EXHIBIT E
REMOTE ACCESS

1. Definitions

(a) "Remote Access" is the act of accessing County Systems from a non-County network infrastructure.

(b) "County Systems," for purposes of this Exhibit, include but are not limited to, all County-owned, leased or managed servers, mainframe computers, desktop computers, laptop computers, handheld devices (including smart phones, wireless PDAs and Pocket PCs), equipment, networks, application systems, databases, software, phone systems, any device with network capabilities (e.g., a workstation with an attached modem, routers, switches, laptop computers, handheld devices), and any other system that stores, processes, and/or transmits County-owned information/data. These items are typically under the direct control and management of the County. "County Systems" also include these items when they are under the control and management of a service provider for use by County, as well as any personally-owned device that an individual has express written permission to use for County purposes.

(c) "County-owned information/data," for purposes of this Exhibit, is any information or data that is transported across a County network, or that resides in a County-owned information system, or on a network or system under the control and management of a service provider for use by County. This information/data is the exclusive property of County unless constitutional provision, State or Federal statute or case law provide otherwise. County-owned information/data does not include a User's personal, non-County business information, communications, data, files and/or software transmitted by or stored on a personally-owned device if that information/data is not transported across a County network or does not reside in a County System or on a network or system under the control and management of a service provider for use by County.

(d) "Contractor employees" includes Contractor's employees, agents, representatives, contractors or subcontractors performing services under this Agreement.

2. Scope of Access

(a) County grants Remote Access privileges (through the method described in section 9) for Contractor to access the following County Systems (collectively referred to as "Designated Systems"), in accordance with the terms of this Agreement:

- IAPro (Sheriff's Office).
- ACeS grievance tracking system (Sheriff's Office).
- Any other Sheriff's Office systems or databases approved by the Sheriff's Office in consultation with the Office of the County Counsel and the Information Security Office. If Contractor is granted Remote Access privileges to additional Sheriff's Office systems or databases, the individuals accessing those additional systems or databases on behalf of Contractor shall sign updated remote access forms reflecting the additional access.

(b) All other forms of access to the Designated Systems, or to any County System that is not specifically named, is prohibited.

(c) Remote Access is granted for the purpose of Contractor providing services and performing its obligations as set forth in this Agreement including, but not limited to, supporting Contractor-installed programs. Any access to the Designated Systems, County-owned information/data, or any other County System or asset that is not specifically authorized under the terms of this Agreement is prohibited and is a material breach that may result in immediate termination of this Agreement for cause and any penalty allowed by law. Contractor may only access the Designated Systems

(d) County will review the scope of Contractor's Remote Access rights periodically.

3. Security Requirements

(a) Contractor will not install any Remote Access capabilities on any County System unless such installation and configuration is approved by the County Information Security Office and meets or exceeds NIST 800-53 standards, or an equivalent industry standard.

(b) Contractor will only remotely access Designated Systems, including access initiated from a County System, if the following conditions are met:

(i) Upon request by an authorized County representative, Contractor will submit documentation verifying its own network security mechanisms to County for County's review and approval. The County reserves the right to advanced written approval of Contractor's security mechanisms prior to Contractor being granted Remote Access.

(ii) The Remote Access method agreed upon pursuant to paragraph 9 must include the following minimum control mechanisms:

(aa) Two-Factor Authentication: An authentication method that requires two of the following three factors to confirm the identity of the user attempting Remote Access. Those factors include: 1) something you possess (e.g., security token and/or smart card); 2) something you know (e.g., a personal identification number (PIN)); or 3) something you are (e.g., fingerprints, retina scan). The only exceptions are County approved County-site-to-Contractor-site Virtual Private Network (VPN) infrastructure.

(bb) County personnel will control authorizations (permissions) to specific systems or networks.

(cc) All Contractor systems used to remotely access County Systems must have industry-standard anti-virus and other security measures that might be required by the County (e.g., software firewall) installed, configured, and activated.

4. Monitoring/Audit

County will monitor access to, and activities on, County Systems, including all Remote Access attempts. Data on all activities will be logged on a County System and will include the date, time, and user identification.

5. Copying, Deleting or Modifying Data

Contractor is prohibited from copying, modifying, or deleting any data contained in or on any County System unless otherwise stated in this Agreement or unless Contractor receives prior written approval from County. This does not include data installed by the Contractor to fulfill its obligations as set forth in this Agreement.

6. Connections to Non-County Networks and/or Systems

Contractor agrees to make every effort to protect data contained on County Systems within Contractor's control from unauthorized access. Prior written approval is required before Contractor may access County Systems from a non-designated system. Such access will use information security protocols that meet or exceed NIST 800-53 standards, or an equivalent industry standard. Remote Access must include the control mechanisms noted in Paragraph 3(b)(ii) above.

7. **Remote Access Contacts**

The following persons are points of contact for purposes of this Exhibit:

Contractor: Julie Ruhlin, julie.ruhlin@oirgroup.com, (562) 335-5443

County: Thomas Nguyen, thomas.d.nguyen@shf.sccgov.org, (408) 808-4643
Leslie Chan, leslie.chan@shf.sccgov.org, (408) 808-4650 (alternate contact)

Either party may change the aforementioned names by providing the other party with no less than three (3) business days prior written notice.

8. Additional Requirements

Contractor agrees to the following:

(a) Only Contractor employees providing services or fulfilling Contractor obligations under this Agreement will be given Remote Access rights.

(b) Any access to Designated Systems, other County Systems and/or County-owned information/data that is not specifically authorized under the terms of this Agreement is prohibited and is a material breach that may result in immediate termination of the Agreement for cause and any other penalty allowed by law.

(c) An encryption method that meets or exceeds Federal Information Processing Standard (FIPS) Publication 140-3 will be used.

(d) Contractor shall protect the integrity of County Systems and County-owned information/data while remotely accessing County resources, and shall report any suspected security incident or concern to the County Service Desk within 24 hours: (408) 970-2222 or support@tss.sccgov.org.

(e) Contractor shall ensure compliance with the terms of this Exhibit and the Exhibit on County Information Technology User Responsibility Statement for Third Parties by all Contractor employees performing services under this Agreement.

(f) Contractor employees have no right, or expectation, of privacy when remotely accessing County Systems or County-owned information/data. County may use audit tools to create detailed records of all remote access attempts and remote access sessions, including User identifier, date, and time of each access attempt.

(g) Contractor employees that have been provided with a County-owned device intended for remote access use, such as a laptop or other Mobile Device, shall ensure that the device is protected from damage, access by third parties, loss, or theft. Contractor employees

shall report loss or theft of such devices to the County Service Desk within 24 hours: (408) 970-2222 or support@tss.sccgov.org.

9. Remote Access Methods

(a) All forms of Remote Access will be made in accordance with mutually agreed upon industry standard protocols and procedures, which must be approved in writing by the County. The remote access solution must conform to County policy and security requirements.

(b) Remote Access Back-Up Method may be used in the event that the primary method of Remote Access is inoperable.

(c) Contractor agrees to abide by the following provisions related to the Primary and (if applicable) Backup Remote Access Methods selected below. (Please mark appropriate box for each applicable Remote Access Method; if a method is not applicable, please check the button marked N/A).

(i) VPN Site-to-Site ○ **Primary** ○ **Backup** ◉ **N/A**

The VPN Site-to-Site method involves a VPN concentrator at both the Contractor site and at the County, with a secure "tunnel" opened between the two concentrators. If using the VPN Site-to-Site Method, Contractor support staff will have access to the Designated Systems from selected network-attached devices at the Contractor site.

(ii) VPN Client Access ○ **Primary** ○ **Backup** ◉ **N/A**

In the VPN Client Access method, a VPN Client (software) is installed on one or more specific devices at the Contractor site, with Remote Access to the County (via a County VPN concentrator) granted from those specific devices only.

An Authentication Token (a physical device or software token that an authorized remote access user is given for user authentication purposes, such as a CryptoCard, RSA token, SecureAuth IdP, Arcot software token, or other such one-time-password mechanism approved by the County Information Security Office) will be issued to the Contractor in order to authenticate Contractor staff when accessing County Designated Systems via this method. The Contractor agrees to the following when issued an Authentication Token:

a. Because the Authentication Token allows access to privileged or confidential information residing on the County's Designated Systems, the Contractor agrees to treat the Authentication Token as it would a signature authorizing a financial commitment on the part of the Contractor.

b. A hardware Authentication Token is a County-owned physical device, and will be labeled as such. The label must remain attached at all times.

c. The Authentication Token is issued to an individual employee of the Contractor and may only be used by the designated individual.

d. The Authentication Token must be kept in the possession of the individual Contractor employee it was issued to or in a secured environment under the direct control of the Contractor, such as a locked office where public or other unauthorized access is not allowed.

e. If the Contractor's remote access equipment is moved to a non-secured site, such as a repair location, the Authentication Token will be kept under Contractor control.

f. If the Authentication Token is misplaced, stolen, or damaged, the Contractor will notify the County TechLink Center by phone within 24 hours.

g. Contractor agrees to use the Authentication Token as part of its normal business operations and for legitimate business purposes only.

h. The Authentication Token will be issued to Contractor following execution of this Agreement. Hardware Authentication Tokens will be returned to the County's Tech Link Center within five (5) business days following contract termination, or upon written request of the County for any reason.

i. Contractor will notify the County's the County TechLink Center within one working day of any change in personnel affecting use and possession of the Authentication Token. The County Service Desk contact information is (408) 970-2222 or support@tss.sccgov.org. Contractor will obtain the Authentication Token from any employee who no longer has a legitimate need to possess the Authentication Token. The County will recoup the cost of any lost or non-returned hardware Authentication.

j. Contractor will not store account or password documentation or PINs with Authentication Tokens.

k. Contractor will ensure all Contractor employees that are issued an Authentication Token will be made aware of and provided with a written copy of the requirements set forth in this Exhibit.

(iii) County-Controlled VPN Client Access ○ **Primary** ○ **Backup** ◉ **N/A**

This form of Remote Access is similar to VPN Client access, except that the County will maintain control of the Authentication Token and a PIN number will be provided to the Contractor for use as identification for Remote Access purposes. When the Contractor needs to access County Designated Systems, the Contractor must first notify the County's Remote Access Contact.

The County's TechLink Center will verify the PIN number provided by the Contractor. After verification of the PIN the County's designee will give the Contractor a one-time password which will be used to authenticate Contractor when accessing the County's Designated Systems. Contractor agrees to the following:

a. Because the PIN number allows access to privileged or confidential information residing on the County's Designated Systems, the Contractor agrees to treat the PIN number as it would a signature authorizing a financial commitment on the part of the Contractor.

b. The PIN number is confidential, County-owned, and will be identified as such.

c. The PIN number must be kept in a secured environment under the direct control of the Contractor, such as a locked office where public or other unauthorized access is not allowed.

d. If the Contractor's remote access equipment is moved to a non-secured site, such as a repair location, the PIN number will be kept under Contractor control.

e. The PIN number can only be released to an authorized employee of the Contractor and may only be used by the designated individual.

f. If the PIN number is compromised or misused, the Contractor will notify the County's designee within one (1) business day.

g. Contractor will use the PIN number as part its normal business operations and for legitimate business purposes only. Any access to Designated Systems, other County Systems, and/or County-owned information/data that is not specifically authorized under the terms of this Agreement is prohibited and is a material breach that may result in immediate termination of the Agreement for cause and any other penalty allowed by law.

h. The PIN number will be issued to Contractor following execution of this Agreement.

i. The PIN number will be inactivated by the County's designee within five (5) business days following contract termination, or as required by the County for any reason.

(iv)County-Controlled Enexity Access ◉ **Primary** ○ **Backup** ○ **N/A**

The County-Controlled Enexity Access method involves using Securelink's Enexity tool installed in the County. County will establish a gateway where Contractor can access the Designated Systems from selected network-attached devices at the County site. County will control the access list for Contractors with access through Enexity gateways.

Signatures of Contractor Employees receiving Authentication Tokens (**Only for VPN Client Access and if tokens issued by County**):

SIGNATURE: _____

[TYPE NAME AND TITLE HERE.]

Date: _____

SIGNATURE: _____

[TYPE NAME AND TITLE HERE.]

Date: _____

SIGNATURE: _____

[TYPE NAME AND TITLE HERE.]

Date: _____

SIGNATURE: _____

[TYPE NAME AND TITLE HERE.]

Date: _____