

EXHIBIT B

BUSINESS AND TECHNICAL REQUIREMENTS

**[NOT ATTACHED TO SAMPLE CONTRACT; SEE
EXHIBIT 10 OF APPENDIX B (REQUIRED FORMS)]**

EXHIBIT C

PRICE SCHEDULE

**[NOT ATTACHED; SEE EXHIBIT 9 OF APPENDIX B
(REQUIRED FORMS)]**

EXHIBIT D

COUNTY'S ADMINISTRATION

COUNTY'S ADMINISTRATION

CONTRACT NO. _____

COUNTY PROJECT DIRECTOR:

Name: _____

Title: _____

Address: _____

Telephone: _____

Facsimile: _____

E-Mail Address: _____

COUNTY PROJECT MANAGER:

Name: _____

Title: _____

Address: _____

Telephone: _____

Facsimile: _____

E-Mail Address: _____

COUNTY CONTRACT PROJECT MONITOR:

Name: _____

Title: _____

Address: _____

Telephone: _____

Facsimile: _____

E-Mail Address: _____

EXHIBIT E

CONTRACTOR'S ADMINISTRATION

CONTRACTOR'S ADMINISTRATION

CONTRACTOR'S NAME: _____

CONTRACT NO: _____

CONTRACTOR'S PROJECT MANAGER:

Name: _____

Title: _____

Address: _____

Telephone: _____

Facsimile: _____

E-Mail Address: _____

CONTRACTOR'S AUTHORIZED OFFICIAL(S)

Name: _____

Title: _____

Address: _____

Telephone: _____

Facsimile: _____

E-Mail Address: _____

Name: _____

Title: _____

Address: _____

Telephone: _____

Facsimile: _____

E-Mail Address: _____

Notices to Contractor shall be sent to the following:

Name: _____

Title: _____

Address: _____

Telephone: _____

Facsimile: _____

E-Mail Address: _____

EXHIBIT F1

CONTRACTOR ACKNOWLEDGEMENT, CONFIDENTIALITY, AND COPYRIGHT ASSIGNMENT AGREEMENT

CONTRACTOR ACKNOWLEDGEMENT, CONFIDENTIALITY, AND COPYRIGHT ASSIGNMENT AGREEMENT

(Note: This certification is to be executed and returned to County with Contractor's executed Contract. Work cannot begin on the Contract until County receives this executed document.)

CONTRACTOR NAME _____ Contract No. _____

GENERAL INFORMATION:

The Contractor referenced above has entered into a contract with the County of Los Angeles to provide certain services to the County. The County requires the Corporation to sign this Contractor Acknowledgement, Confidentiality, and Copyright Assignment Agreement.

CONTRACTOR ACKNOWLEDGEMENT:

Contractor understands and agrees that the Contractor employees, consultants, Outsourced Vendors and independent contractors (Contractor's Staff) that will provide services in the above referenced agreement are Contractor's sole responsibility. Contractor understands and agrees that Contractor's Staff must rely exclusively upon Contractor for payment of salary and any and all other benefits payable by virtue of Contractor's Staff's performance of work under the above-referenced contract.

Contractor understands and agrees that Contractor's Staff are not employees of the County of Los Angeles for any purpose whatsoever and that Contractor's Staff do not have and will not acquire any rights or benefits of any kind from the County of Los Angeles by virtue of my performance of work under the above-referenced contract. Contractor understands and agrees that Contractor's Staff will not acquire any rights or benefits from the County of Los Angeles pursuant to any agreement between any person or entity and the County of Los Angeles.

CONFIDENTIALITY AGREEMENT:

Contractor and Contractor's Staff may be involved with work pertaining to services provided by the County of Los Angeles and, if so, Contractor and Contractor's Staff may have access to confidential data and information pertaining to persons and/or entities receiving services from the County. In addition, Contractor and Contractor's Staff may also have access to proprietary information supplied by other vendors doing business with the County of Los Angeles. The County has a legal obligation to protect all such confidential data and information in its possession, especially data and information concerning health, criminal, and welfare recipient records. Contractor and Contractor's Staff understand that if they are involved in County work, the County must ensure that Contractor and Contractor's Staff, will protect the confidentiality of such data and information. Consequently, Contractor must sign this Confidentiality Agreement as a condition of work to be provided by Contractor's Staff for the County.

Contractor and Contractor's Staff hereby agrees that they will not divulge to any unauthorized person any data or information obtained while performing work pursuant to the above-referenced contract between Contractor and the County of Los Angeles. Contractor and Contractor's Staff agree to forward all requests for the release of any data or information received to County's Project Manager.

Contractor and Contractor's Staff agree to keep confidential all health, criminal, and welfare recipient records and all data and information pertaining to persons and/or entities receiving services from the

CONTRACTOR ACKNOWLEDGEMENT, CONFIDENTIALITY, AND COPYRIGHT ASSIGNMENT AGREEMENT

County, design concepts, algorithms, programs, formats, documentation, Contractor proprietary information and all other original materials produced, created, or provided to Contractor and Contractor's Staff under the above-referenced contract. Contractor and Contractor's Staff agree to protect these confidential materials against disclosure to other than Contractor or County employees who have a need to know the information. Contractor and Contractor's Staff agree that if proprietary information supplied by other County vendors is provided to me during this employment, Contractor and Contractor's Staff shall keep such information confidential.

Contractor and Contractor's Staff agree to report any and all violations of this agreement by Contractor and Contractor's Staff and/or by any other person of whom Contractor and Contractor's Staff become aware.

Contractor and Contractor's Staff acknowledge that violation of this agreement may subject Contractor and Contractor's Staff to civil and/or criminal action and that the County of Los Angeles may seek all possible legal redress.

COPYRIGHT ASSIGNMENT AGREEMENT

Contractor and Contractor's Staff agree that all materials, documents, software programs and documentation, written designs, plans, diagrams, reports, software development tools and aids, diagnostic aids, computer processable media, source codes, object codes, conversion aids, training documentation and aids, and other information and/or tools of all types, developed or acquired by Contractor and Contractor's Staff in whole or in part pursuant to the above referenced contract, and all works based thereon, incorporated therein, or derived therefrom shall be the sole property of the County. In this connection, Contractor and Contractor's Staff hereby assign and transfer to the County in perpetuity for all purposes all my right, title, and interest in and to all such items, including, but not limited to, all unrestricted and exclusive copyrights, patent rights, trade secret rights, and all renewals and extensions thereof. Whenever requested by the County, Contractor and Contractor's Staff agree to promptly execute and deliver to County all papers, instruments, and other documents requested by the County, and to promptly perform all other acts requested by the County to carry out the terms of this agreement, including, but not limited to, executing an assignment and transfer of copyright in a form substantially similar to Exhibit M1, attached hereto and incorporated herein by reference.

The County shall have the right to register all copyrights in the name of the County of Los Angeles and shall have the right to assign, license, or otherwise transfer any and all of the County's right, title, and interest, including, but not limited to, copyrights, in and to the items described above.

Contractor and Contractor's Staff acknowledge that violation of this agreement may subject them to civil and/or criminal action and that the County of Los Angeles may seek all possible legal redress.

NAME OF FIRM: _____

SIGNATURE: _____

DATE: ____/____/____

PRINTED NAME: _____

NAME/TITLE OF ITS AUTHORIZED REPRESENTATIVE: _____

EXHIBIT F2

CONTRACTOR EMPLOYEE ACKNOWLEDGEMENT, CONFIDENTIALITY, AND COPYRIGHT ASSIGNMENT AGREEMENT

CONTRACTOR EMPLOYEE ACKNOWLEDGEMENT, CONFIDENTIALITY, AND COPYRIGHT ASSIGNMENT AGREEMENT

(Note: This certification is to be executed and returned to County with Contractor's executed Contract. Work cannot begin on the Contract until County receives this executed document.)

Contractor Name _____ Contract No. _____

Employee Name _____

GENERAL INFORMATION:

Your employer referenced above has entered into a contract with the County of Los Angeles to provide certain services to the County. The County requires your signature on this Contractor Employee Acknowledgement, Confidentiality, and Copyright Assignment Agreement.

EMPLOYEE ACKNOWLEDGEMENT:

I understand and agree that the Contractor referenced above is my sole employer for purposes of the above-referenced contract. I understand and agree that I must rely exclusively upon my employer for payment of salary and any and all other benefits payable to me or on my behalf by virtue of my performance of work under the above-referenced contract.

I understand and agree that I am not an employee of the County of Los Angeles for any purpose whatsoever and that I do not have and will not acquire any rights or benefits of any kind from the County of Los Angeles by virtue of my performance of work under the above-referenced contract. I understand and agree that I do not have and will not acquire any rights or benefits from the County of Los Angeles pursuant to any agreement between any person or entity and the County of Los Angeles.

I understand and agree that I may be required to undergo a background and security investigation(s). I understand and agree that my continued performance of work under the above-referenced contract is contingent upon my passing, to the satisfaction of the County, any and all such investigations. I understand and agree that my failure to pass, to the satisfaction of the County, any such investigation shall result in my immediate release from performance under this and/or any future contract.

CONFIDENTIALITY AGREEMENT:

I may be involved with work pertaining to services provided by the County of Los Angeles and, if so, I may have access to confidential data and information pertaining to persons and/or entities receiving services from the County. In addition, I may also have access to proprietary information supplied by other vendors doing business with the County of Los Angeles. The County has a legal obligation to protect all such confidential data and information in its possession, especially data and information concerning health, criminal, and welfare recipient records. I understand that if I am involved in County work, the County must ensure that I, too, will protect the confidentiality of such data and information. Consequently, I understand that I must sign this agreement as a condition of my work to be provided by my employer for the County. I have read this agreement and have taken due time to consider it prior to signing.

I hereby agree that I will not divulge to any unauthorized person any data or information obtained while performing work pursuant to the above-referenced contract between my employer and the County of

CONTRACTOR EMPLOYEE ACKNOWLEDGEMENT, CONFIDENTIALITY, AND COPYRIGHT ASSIGNMENT AGREEMENT

Los Angeles. I agree to forward all requests for the release of any data or information received by me to my immediate supervisor.

I agree to keep confidential all health, criminal, and welfare recipient records and all data and information pertaining to persons and/or entities receiving services from the County, design concepts, algorithms, programs, formats, documentation, Contractor proprietary information and all other original materials produced, created, or provided to or by me under the above-referenced contract. I agree to protect these confidential materials against disclosure to other than my employer or County employees who have a need to know the information. I agree that if proprietary information supplied by other County vendors is provided to me during this employment, I shall keep such information confidential.

I agree to report to my immediate supervisor any and all violations of this agreement by myself and/or by any other person of whom I become aware. I agree to return all confidential materials to my immediate supervisor upon completion of this contract or termination of my employment with my employer, whichever occurs first.

COPYRIGHT ASSIGNMENT AGREEMENT

I agree that all materials, documents, software programs and documentation, written designs, plans, diagrams, reports, software development tools and aids, diagnostic aids, computer processable media, source codes, object codes, conversion aids, training documentation and aids, and other information and/or tools of all types, developed or acquired by me in whole or in part pursuant to the above referenced contract, and all works based thereon, incorporated therein, or derived therefrom shall be the sole property of the County. In this connection, I hereby assign and transfer to the County in perpetuity for all purposes all my right, title, and interest in and to all such items, including, but not limited to, all unrestricted and exclusive copyrights, patent rights, trade secret rights, and all renewals and extensions thereof. Whenever requested by the County, I agree to promptly execute and deliver to County all papers, instruments, and other documents requested by the County, and to promptly perform all other acts requested by the County to carry out the terms of this agreement, including, but not limited to, executing an assignment and transfer of copyright in a form substantially similar to Exhibit M1, attached hereto and incorporated herein by reference.

The County shall have the right to register all copyrights in the name of the County of Los Angeles and shall have the right to assign, license, or otherwise transfer any and all of the County's right, title, and interest, including, but not limited to, copyrights, in and to the items described above.

I acknowledge that violation of this agreement may subject me to civil and/or criminal action and that the County of Los Angeles may seek all possible legal redress.

NAME OF FIRM: _____

SIGNATURE: _____

DATE: ____/____/____

PRINTED NAME: _____

NAME/TITLE OF ITS AUTHORIZED REPRESENTATIVE: _____

EXHIBIT F3

**CONTRACTOR NON-EMPLOYEE ACKNOWLEDGEMENT,
CONFIDENTIALITY, AND COPYRIGHT ASSIGNMENT
AGREEMENT**

**CONTRACTOR NON-EMPLOYEE ACKNOWLEDGEMENT, CONFIDENTIALITY,
AND COPYRIGHT ASSIGNMENT AGREEMENT**

(Note: This certification is to be executed and returned to County with Contractor's executed Contract. Work cannot begin on the Contract until County receives this executed document.)

Contractor Name _____ Contract _____

Non-Employee Name _____

GENERAL INFORMATION:

The Contractor referenced above has entered into a contract with the County of Los Angeles to provide certain services to the County. The County requires your signature on this Contractor Non-Employee Acknowledgement, Confidentiality, and Copyright Assignment Agreement.

NON-EMPLOYEE ACKNOWLEDGEMENT:

I understand and agree that the Contractor referenced above has exclusive control for purposes of the above-referenced contract. I understand and agree that I must rely exclusively upon the Contractor referenced above for payment of salary and any and all other benefits payable to me or on my behalf by virtue of my performance of work under the above-referenced contract.

I understand and agree that I am not an employee of the County of Los Angeles for any purpose whatsoever and that I do not have and will not acquire any rights or benefits of any kind from the County of Los Angeles by virtue of my performance of work under the above-referenced contract. I understand and agree that I do not have and will not acquire any rights or benefits from the County of Los Angeles pursuant to any agreement between any person or entity and the County of Los Angeles.

I understand and agree that I may be required to undergo a background and security investigation(s). I understand and agree that my continued performance of work under the above-referenced contract is contingent upon my passing, to the satisfaction of the County, any and all such investigations. I understand and agree that my failure to pass, to the satisfaction of the County, any such investigation shall result in my immediate release from performance under this and/or any future contract.

CONFIDENTIALITY AGREEMENT:

I may be involved with work pertaining to services provided by the County of Los Angeles and, if so, I may have access to confidential data and information pertaining to persons and/or entities receiving services from the County. In addition, I may also have access to proprietary information supplied by other vendors doing business with the County of Los Angeles. The County has a legal obligation to protect all such confidential data and information in its possession, especially data and information concerning health, criminal, and welfare recipient records. I understand that if I am involved in County work, the County must ensure that I, too, will protect the confidentiality of such data and information. Consequently, I understand that I must sign this agreement as a condition of my work to be provided by the above-referenced Contractor for the County. I have read this agreement and have taken due time to consider it prior to signing.

**CONTRACTOR NON-EMPLOYEE ACKNOWLEDGEMENT, CONFIDENTIALITY,
AND COPYRIGHT ASSIGNMENT AGREEMENT**

I hereby agree that I will not divulge to any unauthorized person any data or information obtained while performing work pursuant to the above-referenced contract between the above-referenced Contractor and the County of Los Angeles. I agree to forward all requests for the release of any data or information received by me to the above-referenced Contractor.

I agree to keep confidential all health, criminal, and welfare recipient records and all data and information pertaining to persons and/or entities receiving services from the County, design concepts, algorithms, programs, formats, documentation, Contractor proprietary information, and all other original materials produced, created, or provided to or by me under the above-referenced contract. I agree to protect these confidential materials against disclosure to other than the above-referenced Contractor or County employees who have a need to know the information. I agree that if proprietary information supplied by other County vendors is provided to me, I shall keep such information confidential.

I agree to report to the above-referenced Contractor any and all violations of this agreement by myself and/or by any other person of whom I become aware. I agree to return all confidential materials to the above-referenced Contractor upon completion of this contract or termination of my services hereunder, whichever occurs first.

COPYRIGHT ASSIGNMENT AGREEMENT

I agree that all materials, documents, software programs and documentation, written designs, plans, diagrams, reports, software development tools and aids, diagnostic aids, computer processable media, source codes, object codes, conversion aids, training documentation and aids, and other information and/or tools of all types, developed or acquired by me in whole or in part pursuant to the above referenced contract, and all works based thereon, incorporated therein, or derived therefrom shall be the sole property of the County. In this connection, I hereby assign and transfer to the County in perpetuity for all purposes all my right, title, and interest in and to all such items, including, but not limited to, all unrestricted and exclusive copyrights, patent rights, trade secret rights, and all renewals and extensions thereof. Whenever requested by the County, I agree to promptly execute and deliver to County all papers, instruments, and other documents requested by the County, and to promptly perform all other acts requested by the County to carry out the terms of this agreement, including, but not limited to, executing an assignment and transfer of copyright in a form substantially similar to Exhibit M1, attached hereto and incorporated herein by reference.

The County shall have the right to register all copyrights in the name of the County of Los Angeles and shall have the right to assign, license, or otherwise transfer any and all of the County's right, title, and interest, including, but not limited to, copyrights, in and to the items described above.

I acknowledge that violation of this agreement may subject me to civil and/or criminal action and that the County of Los Angeles may seek all possible legal redress.

NAME OF FIRM: _____

SIGNATURE: _____

DATE: ____/____/____

PRINTED NAME: _____

NAME/TITLE OF ITS AUTHORIZED REPRESENTATIVE: _____

County of Los Angeles
Sheriff's Department

Inmate Commissary and Vending Services
Exhibit F3 – Contractor Non-Employee Acknowledgement,
Confidentiality, and Copyright Assignment Agreement
RFP 525-SH

EXHIBIT G

SAFELY SURRENDERED BABY LAW

THERE'S A BETTER CHOICE. SAFELY SURRENDER YOUR BABY.

Any fire station. Any hospital. Any time.



1.877.222.9723

BabySafeLA.org

No shame | No blame | No names



Some parents of newborns can find themselves in difficult circumstances. Sadly, babies are sometimes harmed or abandoned by parents who feel that they're not ready or able to raise a child. Many of these mothers or fathers are afraid and don't know where to turn for help.

This is why California has a Safely Surrendered Baby Law, which gives parents the choice to legally leave their baby at any hospital or fire station in Los Angeles County.

FIVE THINGS YOU NEED TO KNOW ABOUT BABY SAFE SURRENDER

- 1 Your newborn can be surrendered at any hospital or fire station in Los Angeles County up to 72 hours after birth.
- 2 You must leave your newborn with a fire station or hospital employee.
- 3 You don't have to provide your name.
- 4 You will only be asked to voluntarily provide a medical history.
- 5 You have 14 days to change your mind; a matching bracelet (parent) and anklet (baby) are provided to assist you if you change your mind.

No shame | No blame | No names



ABOUT THE BABY SAFE SURRENDER PROGRAM

In 2002, a task force was created under the guidance of the Children's Planning Council to address newborn abandonment and to develop a strategic plan to prevent this tragedy.

Los Angeles County has worked hard to ensure that the Safely Surrendered Baby Law prevents babies from being abandoned. We're happy to report that this law is doing exactly what it was designed to do: save the lives of innocent babies. Visit BabySafeLA.org to learn more.

No shame | No blame | No names

**ANY FIRE STATION.
ANY HOSPITAL.
ANY TIME.**

**1.877.222.9723
BabySafeLA.org**

**THERE'S A
BETTER CHOICE.
SAFELY SURRENDER
YOUR BABY.**



No shame | No blame | No names





FROM SURRENDER TO ADOPTION: ONE BABY'S STORY

Los Angeles County firefighter Ted and his wife Becki were already parents to two boys. But when they got the call asking if they would be willing to care for a premature baby girl who'd been safely surrendered at a local hospital, they didn't hesitate.

Baby Jenna was tiny, but Ted and Becki felt lucky to be able to take her home. "We had always wanted to adopt," Ted says, "but taking

home a vulnerable safely surrendered baby was even better. She had no one, but now she had us. And, more importantly, we had her."

Baby Jenna has filled the longing Ted and Becki had for a daughter—and a sister for their boys. Because her birth parent safely surrendered her when she was born, Jenna is a thriving young girl growing up in a stable and loving family.

ANSWERS TO YOUR QUESTIONS

Who is legally allowed to surrender the baby?

Anyone with lawful custody can drop off a newborn within the first 72 hours of birth.

Do you need to call ahead before surrendering a baby?

No. A newborn can be surrendered anytime, 24 hours a day, 7 days a week, as long as the parent or guardian surrenders the child to an employee of the hospital or fire station.

What information needs to be provided?

The surrendering adult will be asked to fill out a medical history form, which is useful in caring for the child. The form can be returned later and includes a stamped return envelope. No names are required.

What happens to the baby?

After a complete medical exam, the baby will be released and placed in a safe and loving home, and the adoption process will begin.

What happens to the parent or surrendering adult?

Nothing. They may leave at any time after surrendering the baby.

How can a parent get a baby back?

Parents who change their minds can begin the process of reclaiming their baby within 14 days by calling the Los Angeles County Department of Children and Family Services at (800) 540-4000.

If you're unsure of what to do:

You can call the hotline 24 hours a day, 7 days a week and anonymously speak with a counselor about your options or have your questions answered.

1.877.222.9723 or BabySafeLA.org

English, Spanish and 140 other languages spoken.

ATTACHMENT H

INFORMATION SECURITY AND PRIVACY REQUIREMENTS

INFORMATION SECURITY AND PRIVACY REQUIREMENTS EXHIBIT

The County of Los Angeles (“County”) is committed to safeguarding the Integrity of the County systems, Data, Information and protecting the privacy rights of the individuals that it serves. This Information Security and Privacy Requirements Exhibit (“Exhibit”) sets forth County and Contractor’s commitment and agreement to fulfill each of their obligations under applicable county, state or federal laws, rules, or regulations, as well as applicable industry standards concerning privacy, Data protections, Information Security, Confidentiality, Availability, and Integrity of such Information. The Information Security and privacy requirements and procedures in this Exhibit are to be established by Contractor before the Effective Date of the Contract and maintained throughout the Term of the Contract.

These requirements and procedures are a minimum standard and are in addition to the requirements of the underlying base agreement between the County and Contractor (the “Contractor”) and any other agreements between the parties. However, it is Contractor's sole obligation to: (i) implement appropriate and reasonable measures to secure and protect its systems and all County Information against internal and external Threats and Risks, and (ii) continuously review and revise those measures to address ongoing Threats and Risks. Failure to comply with the minimum requirements and procedures set forth in this Exhibit will constitute a material, non-curable breach of Contract by Contractor, entitling the County, in addition to the cumulative of all other remedies available to it at law, in equity, or under the Contract, to immediately terminate the Contract. To the extent there are conflicts between this Exhibit and the Contract, this Exhibit shall prevail unless stated otherwise.

1. DEFINITIONS

Unless otherwise defined in the Contract, the definitions herein contained are specific to the uses within this Exhibit.

- a. **Availability:** the condition of Information being accessible and usable upon demand by an authorized entity (Workforce Member or process).
- b. **Confidentiality:** the condition that Information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the Information.
- c. **County Information:** all Data and Information belonging to County.
- d. **Data:** a subset of Information comprised of qualitative or quantitative values.
- e. **Incident:** a suspected, attempted, successful, or imminent Threat of unauthorized electronic and/or physical access, use, disclosure, breach, modification, or destruction of information; interference with Information Technology operations; or significant violation of County policy.
- f. **Information:** any communication or representation of knowledge or understanding such as facts, Data, or opinions in any medium or form, including electronic, textual, numerical, graphic, cartographic, narrative, or audiovisual.
- g. **Information Security Policy:** high level statements of intention and direction of an organization used to create an organization’s Information Security Program as formally expressed by its top management.

- h. **Information Security Program:** formalized and implemented Information Security Policies, standards and procedures that are documented describing the program management safeguards and common controls in place or those planned for meeting the County's information security requirements.
- i. **Information Technology:** any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of Data or Information.
- j. **Integrity:** the condition whereby Data or Information has not been improperly modified or destroyed and authenticity of the Data or Information can be ensured.
- k. **Mobile Device Management (MDM):** software that allows Information Technology administrators to control, secure, and enforce policies on smartphones, tablets, and other endpoints.
- l. **Privacy Policy:** high level statements of intention and direction of an organization used to create an organization's Privacy Program as formally expressed by its top management.
- m. **Privacy Program:** A formal document that provides an overview of an organization's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the organization's privacy official and other staff, the strategic goals and objectives of the Privacy Program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.
- n. **Risk:** a measure of the extent to which the County is threatened by a potential circumstance or event, Risk is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs, and (ii) the likelihood of occurrence.
- o. **Threat:** any circumstance or event with the potential to adversely impact the County operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an Information System via unauthorized access, destruction, disclosure, modification of Information, and/or denial of service.
- p. **Vulnerability:** a weakness in a system, application, network or process that is subject to exploitation or misuse.
- q. **Workforce Member:** employees, volunteers, and other persons whose conduct, in the performance of work for the County, is under the direct control of the County, whether or not they are paid by the County. This includes, but may not be limited to, full and part time elected or appointed officials, employees, affiliates, associates, students, volunteers, and staff from third party entities who provide service to the County.

2. INFORMATION SECURITY AND PRIVACY PROGRAMS

- a. **Information Security Program.** Contractor will maintain a company-wide Information Security Program designed to evaluate Risks to the Confidentiality, Availability, and Integrity of County Information covered under the Contract.

Contractor's Information Security Program will include the creation and maintenance of Information Security Policies, standards, and procedures. Information Security Policies, standards, and procedures will be communicated to all Contractor employees in a relevant, accessible, and understandable form and will be regularly reviewed and evaluated to ensure operational effectiveness, compliance with all applicable laws and regulations, and addresses new and emerging Threats and Risks.

Contractor will exercise the same degree of care in safeguarding and protecting County Information that Contractor exercises with respect to its own Information and Data, but in no event less than a reasonable degree of care. Contractor will implement, maintain, and use appropriate administrative, technical, and physical security measures to preserve the Confidentiality, Integrity, and Availability of County Information.

Contractor's Information Security Program will:

- Protect the Confidentiality, Integrity, and Availability of County Information in Contractor's possession or control,
 - Protect against any anticipated Threats or hazards to the Confidentiality, Integrity, and Availability of County Information,
 - Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of County Information,
 - Protect against accidental loss or destruction of, or damage to, County Information, and
 - Safeguard County Information in compliance with any applicable laws and regulations which apply to Contractor.
- b. **Privacy Program.** Contractor will establish and maintain a company-wide Privacy Program designed to incorporate Privacy Policies and practices in its business operations to provide safeguards for Information, including County Information. Contractor's Privacy Program will include the development of, and ongoing reviews and updates to Privacy Policies, guidelines, procedures and appropriate workforce privacy training within its organization. These Privacy Policies, guidelines, procedures, and appropriate training will be provided to all Contractor employees, agents, and volunteers. Contractor's Privacy Policies, guidelines, and procedures will be continuously reviewed and updated for effectiveness and compliance with applicable laws and regulations, and to appropriately respond to new and emerging Threats and Risks. Contractor's Privacy Program will perform ongoing monitoring and audits of operations to identify and mitigate privacy Threats.

Contractor will exercise the same degree of care in safeguarding the privacy of County Information that Contractor exercises with respect to its own Information, but in no event less than a reasonable degree of care. Contractor will implement, maintain, and use appropriate privacy practices and protocols to preserve the Confidentiality of County Information.

Contractor's Privacy Program will include:

- A Privacy Program framework that identifies and ensures that Contractor complies with all applicable laws and regulations,
- External Privacy Policies, and internal privacy policies, procedures and controls to support the privacy program,
- Protections against unauthorized or unlawful access, use, disclosure, alteration, or destruction of County Information,
- A training program that covers Privacy Policies, protocols and awareness,
- A response plan to address privacy Incidents and privacy breaches, and
- Ongoing privacy assessments and audits.

3. PROPERTY RIGHTS TO COUNTY INFORMATION

All County Information is deemed property of the County, and the County will retain exclusive rights and ownership thereto. County Information will not be used by Contractor for any purpose other than as required under the Contract, nor will such or any part of such be disclosed, sold, assigned, leased, or otherwise disposed of, to third parties by Contractor, or commercially exploited or otherwise used by, or on behalf of, Contractor, its officers, directors, employees, or agents. Contractor may assert no lien on or right to withhold from the County, any County Information it receives from, receives addressed to, or stores on behalf of, the County. Notwithstanding the foregoing, Contractor may aggregate, compile, and use County Information in order to improve, develop or enhance the System Software and/or other services offered, or to be offered, by Contractor, provided that: (i) no County Information in such aggregated or compiled pool is identifiable as originating from, or can be traced back to the County, and (ii) such Data or Information cannot be associated or matched with the identity of an individual alone, or linkable to a specific individual. Contractor specifically consents to the County's access to such County Information held, stored, or maintained on any and all devices Contractor owns, leases or possesses.

4. CONTRACTOR'S USE OF COUNTY INFORMATION

Contractor may use County Information only as necessary to carry out its obligations under the Contract. Contractor will collect, maintain, or use County Information only for the purposes specified in the Contract and, in all cases, in compliance with all applicable local, state, and federal laws and regulations governing the collection, maintenance, transmission, dissemination, storage, use, and destruction of County Information, including, but not limited to: (i) any county, state and federal law governing the protection of personal Information, (ii) any county, state and federal security breach notification laws, and (iii) the rules, regulations and directives of the Federal Trade Commission, as amended from time to time.

5. SHARING COUNTY INFORMATION AND DATA

Contractor will not share, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, County Information to a third party for monetary or other valuable consideration.

6. CONFIDENTIALITY

- a. **Confidentiality of County Information.** Contractor agrees that all County Information is Confidential and proprietary to County regardless of whether such Information was disclosed intentionally or unintentionally, or marked as "confidential".
- b. **Disclosure of County Information.** Contractor may disclose County Information only as necessary to carry out its obligations under the Contract, or as required by law, and is prohibited from using County Information for any other purpose without the prior express written approval of County Project Director in consultation with County's Chief Information Security Officer and/or Chief Privacy Officer. If required by a court of competent jurisdiction or an administrative body to disclose County Information, Contractor will notify County Project Director immediately and prior to any such disclosure, to provide the County an opportunity to oppose or otherwise respond to such disclosure, unless prohibited by law from doing so.
- c. **Disclosure Restrictions of Non-Public Information.** While performing Work under the Contract, Contractor may encounter County Non-public Information ("NPI") in the course of performing the Contract, including, but not limited to: licensed technology, drawings,

schematics, manuals, sealed court records, and other materials described and/or identified as “Internal Use”, “Confidential” or “Restricted” as defined in [Board of Supervisors Policy 6.104 – Information Classification Policy](#) as NPI. Contractor will not disclose or publish any County NPI and material received or used in performance of the Contract. This obligation is perpetual.

- d. **Individual Requests.** Contractor will acknowledge any request or instructions from the County regarding the exercise of any individual’s privacy rights provided under applicable federal or state laws. Contractor will have in place appropriate policies and procedures to promptly respond to such requests and comply with any request or instructions from the County within seven Days. If an individual makes a request directly to Contractor involving County Information, Contractor will notify the County within five Days and the County will coordinate an appropriate response, which may include instructing Contractor to assist in fulfilling the request. Similarly, if Contractor receives a privacy or security complaint from an individual regarding County Information, Contractor will notify the County as described in Section 14 SECURITY AND PRIVACY INCIDENTS, and the County will coordinate an appropriate response.
- e. **Retention of County Information.** Contractor will not retain any County Information for any period longer than necessary for Contractor to fulfill its obligations under the Contract and applicable law, whichever is longest.

7. CONTRACTOR EMPLOYEES

Contractor will perform background and security investigation procedures in the manner prescribed in this section unless the Contract prescribes procedures for conducting background and security investigations and those procedures are no less stringent than the procedures described in this section.

To the extent permitted by applicable law, Contractor will screen and conduct background investigations on all Contractor employees and subcontractors as appropriate to their role, with access to County Information for potential security Risks. Such background investigations must be obtained through fingerprints submitted to the California Department of Justice to include state, local, and federal-level review and conducted in accordance with the law, may include criminal and financial history to the extent permitted under the law, and will be repeated on a regular basis. The fees associated with the background investigation will be at the expense of Contractor, regardless of whether the member of Contractor’s staff passes or fails the background investigation. Contractor, in compliance with its legal obligations, will conduct an individualized assessment of their employees, agents, and volunteers regarding the nature and gravity of a criminal offense or conduct; the time that has passed since a criminal offense or conduct and completion of the sentence; and the nature of the access to County Information to ensure that no individual accesses County Information whose past criminal conduct poses a risk or threat to County Information.

Contractor will require all employees, agents, and volunteers to abide by the requirements in this Exhibit, as set forth in the Contract, and sign an appropriate written Confidentiality/non-disclosure agreement with Contractor.

Contractor will supply each of its employees with appropriate, annual training regarding Information Security procedures, Risks, and Threats. Contractor agrees that training will cover, but may not be limited to the following topics:

- a) **Secure Authentication:** The importance of utilizing secure authentication, including proper management of authentication credentials (login name and password) and multi-factor authentication.

- b) **Social Engineering Attacks:** Identifying different forms of social engineering including, but not limited to, phishing, phone scams, and impersonation calls.
- c) **Handling of County Information:** The proper identification, storage, transfer, archiving, and destruction of County Information.
- d) **Causes of Unintentional Information Exposure:** Provide awareness of causes of unintentional exposure of Information such as lost mobile devices, emailing Information to inappropriate recipients, etc.
- e) **Identifying and Reporting Incidents:** Awareness of the most common indicators of an Incident and how such indicators should be reported within the organization.
- f) **Privacy:** Contractor's Privacy Policies and procedures as described in Section 2b. Privacy Program.

Contractor will have an established set of procedures to ensure Contractor's employees promptly report actual and/or suspected breaches of security.

8. SUBCONTRACTORS AND THIRD PARTIES

The County acknowledges that in the course of performing its Services, Contractor may desire or require the use of goods, services, and/or assistance of subcontractors or other third parties or suppliers. The terms of this Exhibit will also apply to all subcontractors and third parties. Contractor or third party will be subject to the following terms and conditions: (i) each subcontractor and third party must agree in writing to comply with and be bound by the applicable terms and conditions of this Exhibit, both for itself and to enable Contractor to be and remain in compliance with its obligations hereunder, including those provisions relating to Confidentiality, Integrity, Availability, disclosures, security, and such other terms and conditions as may be reasonably necessary to effectuate the Contract including this Exhibit; and (ii) Contractor will be and remain fully liable for the acts and omissions of each subcontractor and third party, and fully responsible for the due and proper performance of all Contractor obligations under this Contract.

Contractor will obtain advanced approval from County's Chief Information Security Officer and/or Chief Privacy Officer prior to subcontracting services subject to this Exhibit.

9. STORAGE AND TRANSMISSION OF COUNTY INFORMATION

All County Information will be rendered unusable, unreadable, or indecipherable to unauthorized individuals. Without limiting the generality of the foregoing, Contractor will encrypt all workstations, portable devices (such as mobile, wearables, tablets,) and removable media (such as portable or removable hard disks, floppy disks, USB memory drives, CDs, DVDs, magnetic tape, and all other removable storage media) that store County Information in accordance with Federal Information Processing Standard (FIPS) 140-2 or otherwise approved by County's Chief Information Security Officer.

Contractor will encrypt County Information transmitted on networks outside of Contractor's control with Transport Layer Security (TLS) or Internet Protocol Security (IPSec), at a minimum cipher strength of 128 bit or an equivalent secure transmission protocol or method approved by County's Chief Information Security Officer.

In addition, Contractor will not store County Information in the cloud or in any other online storage provider without written authorization from County's Chief Information Security Officer. All mobile devices storing County Information will be managed by a Mobile Device Management system. Such

system must provide provisions to enforce a password/passcode on enrolled mobile devices. All workstations/Personal Computers (including laptops, 2-in-1s, and tablets) will maintain the latest operating system security patches, and the latest virus definitions. Virus scans must be performed at least monthly. Request for less frequent scanning must be approved in writing by County's Chief Information Security Officer.

10. RETURN OR DESTRUCTION OF COUNTY INFORMATION

Contractor will return or destroy County Information in the manner prescribed in this section unless the Contract prescribes procedures for returning or destroying County Information and those procedures are no less stringent than the procedures described in this section.

- a. **Return or Destruction.** Upon the County's written request, or upon expiration or termination of the Contract for any reason, Contractor will: (i) promptly return or destroy, at the County's option, all originals and copies of all documents and materials it has received containing County Information; or (ii) if return or destruction is not permissible under applicable law, continue to protect such Information in accordance with the terms of the Contract; and (iii) deliver or destroy, at the County's option, all originals and copies of all summaries, records, descriptions, modifications, negatives, drawings, adoptions and other documents or materials, whether in writing or in machine-readable form, prepared by Contractor, prepared under its direction, or at its request, from the documents and materials referred to in Subsection (i) of this Section. For all documents or materials referred to in Subsections (i) and (ii) of this Section that the County requests be returned to the County, Contractor will provide a written attestation on company letterhead certifying that all documents and materials have been delivered to the County. For documents or materials referred to in Subsections (i) and (ii) of this Section that the County requests be destroyed, Contractor will provide an attestation on company letterhead and certified documentation from a media destruction firm consistent with subdivision b (below) of this Section. Upon termination or expiration of the Contract or at any time upon the County's request, Contractor will return all hardware, if any, provided by the County to Contractor. The hardware should be physically sealed and returned via a bonded courier, or as otherwise directed by the County.
- b. **Method of Destruction.** Contractor will destroy all originals and copies by: (i) cross-cut shredding paper, film, or other hard copy media so that the Information cannot be read or otherwise reconstructed; and (ii) purging, or destroying electronic media containing County Information consistent with NIST Special Publication 800-88, "Guidelines for Media Sanitization" such that County Information cannot be retrieved. Contractor will provide an attestation on company letterhead and certified documentation from a media destruction firm, detailing the destruction method used and County Information involved, the date of destruction, and the company or individual who performed the destruction. Such statement will be sent to the designated County Project Director within ten Days of termination or expiration of the Contract or at any time upon the County's request. On termination or expiration of the Contract, the County will return or destroy all Contractor's Information marked as confidential (excluding items licensed to County hereunder, or that provided to County by Contractor hereunder), at the County's option.

11. PHYSICAL AND ENVIRONMENTAL SECURITY

All Contractor facilities that process County Information will be located in secure areas and protected by perimeter security such as barrier access controls (e.g., the use of guards and entry badges) that provide a physically secure environment from unauthorized access, damage, and interference.

All Contractor facilities that process County Information will be maintained with physical and environmental controls (temperature and humidity) that meet or exceed hardware manufacturer's specifications.

12. OPERATIONAL MANAGEMENT, BUSINESS CONTINUITY, AND DISASTER RECOVERY

Contractor will: (i) monitor and manage all of its Information processing facilities, including, without limitation, implementing operational procedures, change management, and Incident response procedures consistent with Section 14 SECURITY AND PRIVACY INCIDENTS; and (ii) deploy adequate anti-malware software and adequate back-up systems to ensure essential business Information can be promptly recovered in the event of a disaster or media failure; and (iii) ensure its operating procedures are adequately documented and designed to protect Information and computer media from theft and unauthorized access.

Contractor must have business continuity and disaster recovery plans. These plans must include a geographically separate back-up data center and a formal framework by which an unplanned event will be managed to minimize the loss of County Information and services. The formal framework includes a defined back-up policy and associated procedures, including documented policies and procedures designed to: (i) perform back-up of data to a remote back-up data center in a scheduled and timely manner, (ii) provide effective controls to safeguard backed-up data, (iii) securely transfer County Information to and from back-up location, (iv) fully restore applications and operating systems, and (v) demonstrate periodic testing of restoration from back-up location. If Contractor makes backups to removable media (as described in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION), all such backups will be encrypted in compliance with the encryption requirements noted above in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION.

13. ACCESS CONTROL

Subject to and without limiting the requirements under Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION, County Information: (i) may only be made available and accessible to those parties explicitly authorized under the Contract or otherwise expressly approved by County Project Director in writing, and (ii) if transferred using removable media (as described in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION) must be sent via a bonded courier and protected using encryption technology designated by Contractor and approved by County's Chief Information Security Officer in writing. The foregoing requirements will apply to back-up media stored by Contractor at off-site facilities.

Contractor will implement formal procedures to control access to County systems, services, and/or Information, including, but not limited to, user account management procedures and the following controls:

- a. Network access to both internal and external networked services will be controlled, including, but not limited to, the use of industry standard and properly configured firewalls,
- b. Operating systems will be used to enforce access controls to computer resources including, but not limited to: multi-factor authentication, use of virtual private networks (VPN), authorization, and event logging,
- c. Contractor will conduct regular, no less often than semi-annually, user access reviews to ensure that unnecessary and/or unused access to County Information is removed in a timely manner,

- d. Applications will include access control to limit user access to County Information and application system functions,
- e. All systems will be monitored to detect deviation from access control policies and identify suspicious activity. Contractor will record, review and act upon all events in accordance with Incident response policies set forth in Section 14 SECURITY AND PRIVACY INCIDENTS, and
- f. In the event any hardware, storage media, or removable media (as described in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION) must be disposed of or sent off-site for servicing, Contractor will ensure all County Information, has been eradicated from such hardware and/or media using industry best practices as discussed in Section 9 STORAGE AND TRANSMISSION OF COUNTY INFORMATION.

14. SECURITY AND PRIVACY INCIDENTS

In the event of a Security or Privacy Incident, Contractor will:

- a. Promptly notify County's Chief Information Security Officer, the Departmental Information Security Officer, and County's Chief Privacy Officer of any Incidents involving County Information, within 24 hours of detection of the Incident. All notifications will be submitted via encrypted email and telephone.

County Chief Information Security Officer and Chief Privacy Officer email

CISO-CPO_Notify@lacounty.gov

Chief Information Security Officer:

Jeffrey Aguilar
Chief Information Security Officer
320 W Temple, 7th Floor
Los Angeles, CA 90012
(213) 253-5600

Chief Privacy Officer:

Lillian Russell
Chief Privacy Officer
320 W Temple, 7th Floor
Los Angeles, CA 90012
(213) 351-5363

Departmental Information Security Officer:

Anthony Cabrera (A/DISO)
Departmental Information Security Officer
12440 Imperial Hwy Suite 400 E
Norwalk, CA 90650

- b. Include the following Information in all notices:
 - i. The date and time of discovery of the Incident,
 - ii. The approximate date and time of the Incident,
 - iii. A description of the type of County Information involved in the reported Incident,
 - iv. A summary of the relevant facts, including a description of measures being taken to respond to and remediate the Incident, and any planned corrective actions as they are identified, and

- v. The name and contact information for the organizations official representative(s), with relevant business and technical information relating to the incident.
- c. Cooperate with the County to investigate the Incident and seek to identify the specific County Information involved in the Incident upon the County's written request, without charge, unless the Incident was caused by the acts or omissions of the County. As Information about the Incident is collected or otherwise becomes available to Contractor, and unless prohibited by law, Contractor will provide Information regarding the nature and consequences of the Incident that are reasonably requested by the County to allow the County to notify affected individuals, government agencies, and/or credit bureaus.
- d. Immediately initiate the appropriate portions of their Business Continuity and/or Disaster Recovery plans in the event of an Incident causing an interference with Information Technology operations.
- e. Assist and cooperate with forensic investigators, the County, law firms, and and/or law enforcement agencies at the direction of the County to help determine the nature, extent, and source of any Incident, and reasonably assist and cooperate with the County on any additional disclosures that the County is required to make as a result of the Incident.
- f. Allow the County or its third-party designee at the County's election to perform audits and tests of Contractor's environment that may include, but are not limited to: interviews of relevant employees, review of documentation, or technical inspection of systems, as they relate to the receipt, maintenance, use, retention, and authorized destruction of County Information.

Notwithstanding any other provisions in the Contract and Exhibit, Contractor will be: (i) liable for all damages and fines, (ii) responsible for all corrective action, and (iii) responsible for all notifications arising from an Incident involving County Information caused by Contractor's weaknesses, negligence, errors, or lack of Information Security or privacy controls or provisions.

15. NON-EXCLUSIVE EQUITABLE REMEDY

Contractor acknowledges and agrees that due to the unique nature of County Information there can be no adequate remedy at law for any breach of its obligations hereunder, that any such breach may result in irreparable harm to the County, and therefore, that upon any such breach, the County will be entitled to appropriate equitable remedies, and may seek injunctive relief from a court of competent jurisdiction without the necessity of proving actual loss, in addition to whatever remedies are available within law or equity. Any breach of Section 6 CONFIDENTIALITY constitutes a material breach and will be grounds for immediate termination of the Contract at the exclusive discretion of the County.

16. AUDIT AND INSPECTION

- a. **Self-Audits.** Contractor will periodically conduct audits, assessments, testing of the system of controls, and testing of Information Security and privacy procedures, including penetration testing, intrusion detection, and firewall configuration reviews. These periodic audits will be conducted by staff certified to perform the specific audit in question at Contractor's sole cost and expense through either: (i) an internal independent audit function, (ii) a nationally recognized, external, independent auditor, or (iii) another independent auditor approved by County.

Contractor will have a process for correcting control deficiencies that have been identified in the periodic audit, including follow up documentation providing evidence of such corrections. Contractor will provide the audit results and any corrective action documentation to the County promptly upon its completion at the County's request. With respect to any other report,

certification, or audit or test results prepared or received by Contractor that contains any County Information, Contractor will promptly provide the County with copies of the same upon the County's reasonable request, including identification of any failure or exception in Contractor's Information systems, products, and services, and the corresponding steps taken by Contractor to mitigate such failure or exception. Any reports and related materials provided to the County pursuant to this Section will be provided at no additional charge to the County.

- b. **County Requested Audits.** At its own expense, the County, or an independent third-party auditor commissioned by the County, will have the right to audit Contractor's infrastructure, security and privacy practices, Data center, services and/or systems storing or processing County Information via an onsite inspection at least once a year. Upon the County's request, Contractor will complete a questionnaire regarding Contractor's Information Security and/or program. The County will pay for the County requested audit unless the auditor finds that Contractor has materially breached this Exhibit, in which case Contractor will bear all costs of the audit; and if the audit reveals material non-compliance with this Exhibit, the County may exercise its termination rights underneath the Contract.

Such audit will be conducted during Contractor's normal business hours with reasonable advance notice, in a manner that does not materially disrupt or otherwise unreasonably and adversely affect Contractor's normal business operations. The County's request for the audit will specify the scope and areas (e.g., Administrative, Physical, and Technical) that are subject to the audit and may include, but are not limited to physical controls inspection, process reviews, policy reviews, evidence of external and internal Vulnerability scans, penetration test results, evidence of code reviews, and evidence of system configuration and audit log reviews. It is understood that the results may be filtered to remove the specific Information of other Contractor customers such as IP address, server names, etc. Contractor will cooperate with the County in the development of the scope and methodology for the audit, and the timing and implementation of the audit. This right of access will extend to any regulators with oversight of the County. Contractor agrees to comply with all reasonable recommendations that result from such inspections, tests, and audits within reasonable timeframes.

When not prohibited by regulation, Contractor will provide to the County a summary of: (i) the results of any security audits, security reviews, or other relevant audits, conducted by Contractor or a third party; and (ii) corrective actions or modifications, if any, Contractor will implement in response to such audits.

17. CYBER LIABILITY INSURANCE

Contractor will secure and maintain cyber liability insurance coverage in the manner prescribed in this section unless the Contract prescribes cyber liability insurance coverage provisions and those provisions are no less stringent than those described in this section.

Contractor will secure and maintain cyber liability insurance coverage with limits of at least **\$2,000,000** per occurrence and in the aggregate during the term of the Contract, including coverage for: network security liability; privacy liability; privacy regulatory proceeding defense, response, expenses and fines; technology professional liability (errors and omissions); privacy breach expense reimbursement (liability arising from the loss or disclosure of County Information no matter how it occurs); system breach; denial or loss of service; introduction, implantation, or spread of malicious software code; unauthorized access to or use of computer systems; and Data/Information loss and business interruption; any other liability or risk that arises out of the Contract. Contractor will add the County as an additional insured to its cyber liability insurance policy and provide to County certificates of insurance evidencing the foregoing upon the County's request. The procuring of the insurance described herein, or delivery of the certificates of insurance described herein, will

not be construed as a limitation upon Contractor's liability or as full performance of its indemnification obligations hereunder. No exclusion/restriction for unencrypted portable devices/media may be on the policy.

18. PRIVACY AND SECURITY INDEMNIFICATION

In addition to the indemnification provisions in the Contract, Contractor agrees to indemnify, defend, and hold harmless the County, its Special Districts, elected and appointed officers, agents, employees, and volunteers from and against any and all claims, demands liabilities, damages, judgments, awards, losses, costs, expenses or fees including reasonable attorneys' fees, accounting and other expert, consulting or professional fees, and amounts paid in any settlement arising from, connected with, or relating to:

- Contractor's violation of any federal and state laws in connection with its accessing, collecting, processing, storing, disclosing, or otherwise using County Information;
- Contractor's failure to perform or comply with any terms and conditions of this Contract or related agreements with the County; and/or,
- Any Information loss, breach of Confidentiality, or Incident involving any County Information that occurs on Contractor's systems or networks (including all costs and expenses incurred by County to remedy the effects of such loss, breach of Confidentiality, or Incident, which may include (i) providing appropriate notice to individuals and governmental authorities, (ii) responding to individuals' and governmental authorities' inquiries, (iii) providing credit monitoring to individuals, and (iv) conducting litigation and settlements with individuals and governmental authorities).

Notwithstanding the preceding sentences, the County will have the right to participate in any such defense at its sole cost and expense, except that in the event contractor fails to provide the County with a full and adequate defense, as determined by the County in its sole judgment, the County will be entitled to retain its own counsel, including, without limitation, County Counsel, and to reimbursement from contractor for all such costs and expenses incurred by the County in doing so. Contractor will not have the right to enter into any settlement, agree to any injunction or other equitable relief, or make any admission, in each case, on behalf of the County without the County's prior written approval.

ADDENDUM A: CONTRACTOR HARDWARE CONNECTING TO COUNTY SYSTEMS

Notwithstanding any other provisions in the Contract, Contractor will ensure the following provisions and security controls are established for any and all systems or hardware provided under the Contract.

- a. **Inventory:** Contractor must actively manage, including through inventory, tracking, loss prevention, replacement, updating, and correcting, all hardware devices covered under the Contract. Contractor must be able to provide such management records to County at inception of the Contract and upon request.
- b. **Access Control:** Contractor agrees to manage access to all systems or hardware covered under the Contract. This includes industry-standard management of administrative privileges including, but not limited to, maintaining an inventory of administrative privileges, changing default passwords, use of unique passwords for each individual accessing systems or hardware under the Contract, and minimizing the number of individuals with administrative privileges to those strictly necessary. Prior to effective date of the Contract, Contractor must document their access control plan for systems or hardware covered under the Contract and provide such plan to the Department Information Security Officer (DISO) who will consult with County's Chief Information Security Officer (CISO) for review and approval. Contractor must modify and/or implement such plan as directed by the DISO and CISO.
- c. **Operating System and Equipment Hygiene:** Contractor agrees to ensure that systems or hardware will be kept up to date, using only the most recent and supported operating systems, applications, and programs, including any patching or other solutions for vulnerabilities, within 90 Days of the release of such updates, upgrades, or patches. Contractor agrees to ensure that the operating system is configured to eliminate any unnecessary applications, services and programs. If for some reason Contractor cannot do so within 90 Days, Contractor must provide a Risk assessment to County's Chief Information Security Officer (CISO).
- d. **Vulnerability Management:** Contractor agrees to continuously acquire, assess, and take action to identify and remediate vulnerabilities within the Systems and Hardware covered under the Contract. If such vulnerabilities cannot be addressed, Contractor must provide a Risk assessment to the Department Information Security Officer (DISO) who will consult with County's Chief Information Security Officer (CISO). County's CISO must approve the Risk acceptance and Contractor accepts liability for Risks that result to the County for exploitation of any un-remediated vulnerabilities.
- e. **Media Encryption:** Throughout the duration of the Contract, Contractor will encrypt all workstations, portable devices (e.g., mobile, wearables, tablets,) and removable media (e.g., portable or removable hard disks, floppy disks, USB memory drives, CDs, DVDs, magnetic tape, and all other removable storage media) associated with systems and hardware provided under the Contract in accordance with Federal Information Processing Standard (FIPS) 140-2 or otherwise required or approved by County's Chief Information Security Officer (CISO).
- f. **Malware Protection:** Contractor will provide and maintain industry-standard endpoint antivirus and antimalware protection on all systems and hardware as approved or required by the Department Information Security Officer (DISO) who will consult with the County's Chief Information Security Officer (CISO) to ensure provided hardware is free, and remains free of malware. Contractor agrees to provide the County documentation proving malware protection status upon request.

ADDENDUM C: APPLICATION SOURCE CODE REPOSITORY

The Contractor shall manage the source code in the manner prescribed in this Addendum unless the Contract prescribes procedures for managing the source code and those procedures are no less stringent than the procedures described in this addendum.

- a. **County Application Source Code.** To facilitate the centralized management, reporting, collaboration, and continuity of access to the most current production version of application source code, all code, artifacts, and deliverables produced under this Contract, (hereinafter referred to as “County Source Code”) shall be version controlled, stored, and delivered on a single industry-standard private Git repository, provided, managed, and supported by the County. Upon commencement of the contract period, the Contractor will be granted access to the County’s private Git repository.
- b. **Git Repository.** The Contractor will use the County Git repository during the entire lifecycle of the project from inception to final delivery. The Contractor will create and document design documents, Data flow diagrams, security diagrams, configuration settings, software or hardware requirements and specifications, attribution to third-party code, libraries and all dependencies, and any other documentation related to all County Source Code and corresponding version-controlled documentation within the Git repository. This documentation must include an Installation Guide and a User Guide for the final delivered source code such that County may download, install, and make full functional use of the delivered code as specified and intended.

ATTACHMENT H.1

DEPARTMENTAL INFORMATION SECURITY REQUIREMENTS

ATTACHMENT H.1

DEPARTMENTAL INFORMATION SECURITY REQUIREMENTS

This Attachment H.1 sets forth information security procedures to be established by Contractor before the effective date of the Contract and maintained throughout the term of the Contract. These procedures are in addition to the requirements of the Contract. They present a minimum standard only. However, it is Contractor's sole obligation to: (i) implement appropriate measures to secure its systems and data, including Personal Information, Protected Health Information and County's Confidential Information, against internal and external threats and risks; and (ii) continuously review and revise those measures to address ongoing threats and risks. Failure to comply with the minimum standards set forth in this Attachment H.1 will constitute a material, non-curable breach of the Contract by Contractor, entitling County, in addition to and cumulative of all other remedies available to it at law, in equity, or under the Contract, to immediately terminate the Contract. Unless specifically defined in this Attachment H.1, capitalized terms shall have the meanings set forth in the Contract.

1. SECURITY POLICY

Contractor shall establish and maintain a formal, documented, mandated, company-wide information security program, including security policies, standards and procedures (collectively "**Information Security Policy**"). The Information Security Policy will be communicated to all Contractor personnel in a relevant, accessible, and understandable form and will be regularly reviewed and evaluated to ensure its operational effectiveness, compliance with all applicable laws and regulations, and to address new threats and risks.

2. PERSONNEL AND CONTRACTOR PROTECTIONS

Contractor shall screen and conduct background checks on all Contractor personnel who will have access to County's Confidential Information, including Personally Identifiable Information and Protected Health Information, for potential security risks and require all employees and contractors to sign an appropriate written confidentiality/non-disclosure agreement. All agreements with third parties involving access to Contractor's systems and data, including all outsourcing arrangements and maintenance and support agreements (including facilities maintenance), shall specifically address security risks, controls, and procedures for information systems. Contractor shall supply each of its Contractor personnel with appropriate, ongoing training regarding information security procedures, risks, and threats. Contractor shall have an established set of procedures to ensure Contractor personnel promptly report actual and/or suspected breaches of security.

3. REMOVABLE MEDIA

Except in the context of Contractor's routine back-ups or as otherwise specifically authorized by County in writing, Contractor shall institute strict security controls, including encryption of Removable Media (as defined below), to prevent transfer of Personally Identifiable Information and Protected Health Information to any form of Removable Media. For purposes of this Attachment H.1, "**Removable Media**" means portable or removable hard disks, floppy disks, USB memory drives, zip disks, optical disks, CDs, DVDs, digital film, digital cameras, memory cards (e.g., Secure Digital (SD), Memory Sticks (MS), CompactFlash (CF), SmartMedia (SM), MultiMediaCard (MMC), and xD-Picture Card (xD)), magnetic tape, and all other removable data storage media.

4. STORAGE, TRANSMISSION AND DESTRUCTION OF PROTECTED HEALTH INFORMATION

All Protected Health Information shall be rendered unusable, unreadable, or indecipherable to unauthorized individuals in accordance with HIPAA, as amended and supplemented by the HITECH Act. Without limiting the generality of the foregoing, Contractor will encrypt all workstations and portable devices (e.g., mobile, wearables, tablets, thumb drives, external hard drives) that store County's Confidential Information (including Protected Health Information) in accordance with Federal Information Processing Standard (FIPS) 140-2. Contractor will encrypt County's Confidential Information transmitted on networks outside of Contractor's control with Secure Socket Layer (SSL or TLS), at a minimum, cipher strength of 256 bit. If County's Confidential Information is no longer required to be retained by Contractor under the Contract and applicable law, Contractor shall destroy such information by: (a) shredding or otherwise destroying paper, film, or other hard copy media so that the information cannot be read or otherwise cannot be reconstructed; and (b) clearing, purging, or destroying electronic media containing Protected Health Information consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization such that the Protected Health Information cannot be retrieved. Contractor will not store County's Confidential Information (including Protected Health Information) in the cloud or in any other online storage provider.

All mobile devices storing County's Confidential Information (including Protected Health Information) must be managed by a Mobile Device Management system. All workstations/PCs will maintain the latest security patches and have the latest virus definitions. Virus scans should be run daily and logged.

5. DATA CONTROL; MEDIA DISPOSAL AND SERVICING

Subject to and without limiting the requirements under Section 4 (Storage, Transmission and Destruction of Protected Health Information), Personally Identifiable Information, Protected Health Information, and County's Confidential Information: (i) may only be made available and accessible to those parties explicitly authorized under the Contract or otherwise expressly approved by County in writing; (ii) if transferred across the Internet, any wireless network (e.g., cellular, 802.11x, or similar technology), or other public or shared networks, must be protected using appropriate encryption technology as designated or Approved by County Project Director in writing; and (iii) if transferred using Removable Media (as defined above) must be sent via a bonded courier or protected using encryption technology designated by Contractor and approved by County in writing. The foregoing requirements shall apply to back-up data stored by Contractor at off-site facilities. In the event any hardware, storage media, or Removable Media must be disposed of or sent off-site for servicing, Contractor must ensure all County's Confidential Information, including Personally Identifiable Information and Protected Health Information, has been cleared, purged, or scrubbed from such hardware and/or media using industry best practices (e.g., NIST Special Publication 800-88, Guidelines for Media Sanitization).

6. HARDWARE RETURN

Upon termination or expiration of the Contract at any time upon County's request, Contractor shall return all hardware, if any, provided by County containing Personally Identifiable Information, Protected Health Information, or County's Confidential Information to County. The Personally Identifiable Information, Protected Health Information, and County's Confidential Information should not be removed or altered in any way. The hardware should be physically sealed and returned via a bonded courier or as otherwise directed by County. In the event the hardware containing County's Confidential Information or Personally Identifiable Information is owned by Contractor or a third party, a notarized statement, detailing the destruction method used and the data sets involved, the date of destruction, and the company and/or individual who performed the destruction will be sent to a designated County security representative within fifteen (15) days of termination or expiration of the Contract or at any time upon County's request. Contractor's destruction or erasure of Personal

Information and Protected Health Information pursuant to this Section shall be in compliance with industry Best Practices (e.g., NIST Special Publication 800-88, Guidelines for Media Sanitization).

7. PHYSICAL AND ENVIRONMENTAL SECURITY

Contractor facilities that process Personally Identifiable Information, Protected Health Information, or County's Confidential Information must be housed in secure areas and protected by perimeter security such as barrier access controls (e.g., the use of guards and entry badges) that provide a physically secure environment from unauthorized access, damage, and interference.

8. COMMUNICATIONS AND OPERATIONAL MANAGEMENT

Contractor must: (i) monitor and manage all of its information processing facilities, including without limitation, implementing operational procedures, change management and incident response procedures; (ii) deploy adequate anti-viral software and adequate back-up facilities to ensure essential business information can be promptly recovered in the event of a disaster or media failure; and (iii) ensure its operating procedures will be adequately documented and designed to protect information, computer media, and data from theft and unauthorized access.

9. ACCESS CONTROL

Contractor shall implement formal procedures to control access to its systems, services, and data, including but not limited to, user account management procedures and the following controls:

- a. Network access to both internal and external networked services shall be controlled, including but not limited to, the use of properly configured firewalls;
- b. Operating systems will be used to enforce access controls to computer resources including but not limited to, authentication, authorization, and event logging;
- c. Applications will include access control to limit user access to information and application system functions; and
- d. All systems will be monitored to detect deviation from access control policies and identify suspicious activity. Contractor shall record, review and act upon all events in accordance with incident response policies set forth below.

10. SECURITY INCIDENT

A "Security Incident" shall mean the attempted or successful unauthorized access, use, disclosure, modification or interference with system operations in an information system.

- a. Contractor will promptly notify (but in no event more than twenty-four (24) hours after the detection of a Security Incident) the designated County security contact by telephone and subsequently via written letter of any potential or actual security attacks or Security Incidents.
- b. The notice shall include the approximate date and time of the occurrence and a summary of the relevant facts, including a description of measures being taken to address the occurrence. A Security Incident includes instances in which internal personnel access systems in excess of their user rights or use the systems inappropriately.
- c. Contractor will provide a report of all Security Incidents noting the corrective actions taken to mitigate the Security Incidents. This will be provided via a written letter to the County security representative as part of Contractor's annual audit or as reasonably requested by County. County or its third party designee may, but is not obligated, perform audits and security tests of Contractor's environment that may include, but are not limited to, interviews of relevant personnel, review of documentation, or technical inspection of systems, as they relate to the receipt, maintenance, use, retention, and authorized destruction of Personally Identifiable Information, Protected Health Information, and County's Confidential Information.

- d. County reserves the right to view, upon request, summary results (i.e., the number of high, medium and low vulnerabilities) and related corrective action schedule for which Contractor has undertaken on its behalf to assess Contractor's own network security. If requested, copies of these summary results and corrective action schedules will be sent to the County security contact.

11. CONTRACTOR SELF AUDIT

As part of Contractor's annual audit or upon County's request, Contractor will provide to County a summary of: (1) the results of any security audits, security reviews, or other relevant audits listed below, conducted by Contractor or a third party; and (2) the corrective actions or modifications, if any, Contractor will implement in response to such audits.

Relevant audits conducted by Contractor as of the Effective Date must include:

- a. ISO 27001:2013 (Information Security Management) or FDA's Quality System Regulation, etc. – Contractor-wide. A full recertification is conducted every three (3) years with surveillance audits annually.
 - (i) **External Audit** – Audit conducted by non-Contractor personnel, to assess Contractor's level of compliance to applicable regulations, standards, and contractual requirements.
 - (ii) **Internal Audit** – Audit conducted by qualified Contractor Personnel (or contracted designee) not responsible for the area of review, of Contractor organizations, operations, processes, and procedures, to assess compliance to and effectiveness of Contractor's Quality System ("CQS") in support of applicable regulations, standards, and requirements.
 - (iii) **Supplier Audit** – Quality audit conducted by qualified Contractor Personnel (or contracted designee) of product and service suppliers contracted by Contractor for internal or Contractor client use.
 - (iv) **Detailed findings** – are not published externally, but a summary of the report findings, and corrective actions, if any, will be made available to County as provided above and the ISO certificate is published on Buck Consultants LLC.
- b. SSAE-16 (formerly known as SAS -70 II) – As to the Hosting Services only:
 - (i) Audit spans a full twelve (12) months of operation and is produced annually.
 - (ii) The resulting detailed report is available to County.
 - (iii) Detailed findings are not published externally, but a summary of the report findings, and corrective actions, if any, will be made available to County as provided above.

12. SECURITY AUDITS

In addition to the audits described in Section 11 (Contractor Self Audit), during the term of this Contract, County or its third-party designee may annually, or more frequently as agreed in writing by the parties, request a security audit of Contractor's data center and systems. The audit will take place at a mutually agreed time by the parties, but in no event on a date more than ninety (90) days from the date of the request by County. County's request for security audit will specify the areas (e.g., Administrative, Physical and Technical) that are subject to the audit and may include but not limited to physical controls, inspection, process reviews, policy reviews, evidence of external and internal vulnerability scans, evidence of code reviews, and evidence of system configuration and audit log reviews. County shall pay for all third-party costs associated with the audit. It is understood that summary data of the results must be filtered to remove the specific information of other Contractor customers such as IP address, server names, etc.

Contractor shall cooperate with County in the development of the scope and methodology for the audit, and the timing and implementation of the audit. Any of the County's regulators shall have the same

right upon request, to request an audit as described above. Contractor agrees to comply with all reasonable recommendations that result from such inspections, tests, and audits within reasonable timeframes.

13. CONFIDENTIALITY

- a. **Confidential Information.** Contractor agrees that all information supplied by its affiliates and agents to the County including, without limitation, (a) any information relating to County's customers, patients, business partners, or personnel; (b) Personally Identifiable Information (as defined below); and (c) any Protected Health Information under The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and The Health Information Technology for Economic and Public Health Act (HITECH), will be deemed confidential and proprietary to the County, regardless of whether such information was disclosed intentionally or unintentionally or marked as "confidential" or "proprietary" ("Confidential Information"). To be deemed "Confidential Information", trade secrets and mask works must be plainly and prominently marked with restrictive legends.
- b. **County Data.** All of County's Confidential Information, data, records and information of County to which Contractor has access, or otherwise provided to Contractor under this Contract ("County Data"), is and will remain the property of County and County retains exclusive rights and ownership thereto. The County Data may not be used by Contractor for any purpose other than as required under this Contract, nor may such data or any part of such data be disclosed, sold, assigned, leased or otherwise disposed of to third parties by Contractor or commercially exploited or otherwise used by or on behalf of Contractor, its officers, directors, employees, or agents.
- c. **Non-Exclusive Equitable Remedy.** Subject to the limitations and other applicable provisions set forth in the Contract, Contractor acknowledges and agrees that due to the unique nature of Confidential Information there can be no adequate remedy at law for any breach of its obligations hereunder, that any such breach or threatened breach may result in irreparable harm to County, and therefore, that upon any such breach or any threat thereof, County will be entitled to appropriate equitable remedies, and may seek injunctive relief from a court of competent jurisdiction without the necessity of proving actual loss, in addition to whatever remedies either of them might have at law or equity. Any breach of this Section 13 (Confidentiality) shall constitute a material breach of this Contract and be grounds for immediate termination of this Contract in the exclusive discretion of the County.
- d. **Personally Identifiable Information.** "Personally Identifiable Information" shall mean any information that identifies a person, including but not limited to, name, address, email address, passwords, account numbers, social security numbers, credit card information, personal financial or healthcare information, personal preferences, demographic data, marketing data, credit data, or any other identification data. For the avoidance of doubt, Personally Identifiable Information shall include, but not be limited to, all "nonpublic personal information," as defined under the Gramm-Leach-Bliley Act (15 United States Code ("U.S.C.") §6801 et seq.), Protected Health Information, and "Personally Identifiable Information" as that term is defined in EU Data Protection Directive (Directive 95/46/EEC) on the protection of individuals with regard to processing of personal data and the free movement of such data.
 - i. **Personally Identifiable Information.** In connection with this Contract and performance of the services, Contractor may be provided or obtain, from County or otherwise, Personally Identifiable Information pertaining to County's current and prospective personnel, directors and officers, agents, investors, patients, and customers and may need to process such Personally Identifiable Information and/or transfer it, all subject to the restrictions set forth in this Contract and otherwise in compliance with all applicable foreign and domestic laws and regulations for the sole purpose of performing the services.

- ii. **Treatment of Personally Identifiable Information.** Without limiting any other warranty or obligations specified in this Contract, and in particular the Confidentiality provisions of the Contract, during the term of this Contract and thereafter in perpetuity, Contractor will not gather, store, log, archive, use, or otherwise retain any Personally Identifiable Information in any manner and will not disclose, distribute, sell, share, rent, or otherwise retain any Personally Identifiable Information to any third party, except as expressly required to perform its obligations in this Contract or as Contractor may be expressly directed in advance in writing by County. Contractor represents and warrants that Contractor will use and process Personally Identifiable Information only in compliance with (a) this Contract, (b) County's then current privacy policy, and (c) all applicable local, state, and federal laws and regulations (including, but not limited to, current and future laws and regulations relating to spamming, privacy, confidentiality, data security, and consumer protection).
- iii. **Retention of Personally Identifiable Information.** Contractor will not retain any Personally Identifiable Information for any period longer than necessary for Contractor to fulfill its obligations under this Contract. As soon as Contractor no longer needs to retain such Personally Identifiable Information in order to perform its duties under this Contract, Contractor will promptly return or destroy or erase all originals and copies of such Personally Identifiable Information.
- e. **Return of Confidential Information.** On County's written request or upon expiration or termination of this Contract for any reason, Contractor will promptly: (a) return or destroy, at County's option, all originals and copies of all documents and materials it has received containing County's Confidential Information; (b) if return or destruction is not permissible under applicable law, continue to protect such information in accordance with the terms of this Contract; and (c) deliver or destroy, at County's option, all originals and copies of all summaries, records, descriptions, modifications, negatives, drawings, adoptions and other documents or materials, whether in writing or in machine-readable form, prepared by Contractor, prepared under its direction, or at its request, from the documents and materials referred to in Subsection 13(a), and provide a notarized written statement to County certifying that all documents and materials referred to in Subsections 13(a) and (b) above have been delivered to County or destroyed, as requested by County. On termination or expiration of this Contract, County shall return or destroy all Contractor's Confidential Information (excluding items licensed to County hereunder or that are required for use of the Deliverables and/or the Software), at Contractor's option.

ATTACHMENT H.2

COMPLIANCE WITH DEPARTMENTAL ENCRYPTION REQUIREMENTS

ATTACHMENT H.2

COMPLIANCE WITH DEPARTMENTAL ENCRYPTION REQUIREMENTS

Contractor is required to provide information about its encryption practices with respect to Personal Information, Protected Health Information, Medical Information and any other information described in Paragraph 7.6.5 (Protection of Electronic County Information - Data Encryption) of the Contract by completing this Attachment H.2. By signing this Attachment H.2, Contractor certifies that it will be in compliance with the Los Angeles County Board of Supervisors Policy 5.200 (Contractor Protection of Electronic County Information) upon the Effective Date and during the Term of the Contract.

COMPLIANCE QUESTIONS	DOCUMENTATION AVAILABLE			
	YES	NO	YES	NO
1) Will County data stored on your workstation(s) be encrypted?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2) Will County data stored on your laptop(s) be encrypted?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3) Will County data stored on removable media be encrypted?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4) Will County data be encrypted when transmitted?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5) Will Contractor maintain a copy of any validation/attestation reports generated by its encryption tools?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6) Will County data be stored on remote servers*? <i>*cloud storage, Software-as-a-Service or SaaS</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

NAME OF FIRM: _____

NAME/TITLE OF AUTHORIZED REPRESENTATIVE: _____

SIGNATURE: _____

DATE: _____