INFORMATION SECURITY AND PRIVACY REQUIREMENTS FOR CONTRACTS

The County of Los Angeles ("County") is committed to safeguarding the Integrity of County Systems, Data, and Information, and to protecting the privacy rights of the individuals that it serves. This Information Security and Privacy Requirements, Attachment 1 (Attachment) to Exhibit K (Attestation Regarding Information Security Requirement ("Attachment") sets forth the County and the Contractor's commitment and agreement to fulfill each of their obligations under applicable 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 Attachment are to be established by the 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 "Contract") and any other agreements between the parties. However, it is the 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 Attachment will constitute a material, non-curable breach of Contract by the 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 Attachment and the Contract, this Attachment will prevail unless stated otherwise.

1. DEFINITIONS

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

a. Artificial Intelligence (AI): technologies used to simulate human intelligence and are programmed to think like humans and mimic their actions in the collection, design, interoperability, and management of data.

b. Availability: the condition of Information being accessible and usable upon demand by an authorized entity (user, process, device).

c. Confidentiality: the condition that Information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the Information.

d. County Information: all Data and Information belonging to the County.

e. Data: a subset of Information comprised of qualitative or quantitative values.

f. 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.

g. 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.

h. 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.

i. 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.

j. 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.

k. Integrity: the condition whereby Data or Information has not been improperly modified or destroyed and authenticity of the Data or Information can be ensured.

l. Mobile Device Management (MDM): software that allows Information Technology administrators to control, secure, and enforce policies on smartphones, tablets, and other endpoints.

m. 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.

n. 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.

o. 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.

p. Threat: any circumstance or event with the potential to adversely impact 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.

q. Vulnerability: a weakness in a system, application, network or process that is subject to exploitation or misuse.

r. Workforce Member: employees, volunteers, and other persons whose conduct, in the performance of work for Los Angeles County, is under the direct control of Los Angeles County, whether or not they are paid by Los Angeles 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. The Contractor must maintain a company-wide Information Security Program designed to evaluate Risks to the Confidentiality, Availability, and Integrity of the County Information covered under this Contract.

Contractor's Information Security Program must 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.

The Contractor must exercise the same degree of care in safeguarding and protecting County information that the Contractor exercises with respect to its own information and data and, at a minimum, a reasonable degree of care. The Contractor will implement, maintain, and use appropriate administrative, technical, and physical security measures to preserve the confidentiality, availability, and integrity, of County information.

The Contractor's Information Security Program must:

- Prohibit the implementation or use of AI technologies for data management; including data collection, data storage, data retrieval, data sharing, and without written approval from the Department of Mental Health's Chief Information Officer and Information Security Officer;

- Protect the Confidentiality, Integrity, and Availability of County information in the 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 the Contractor.

b. Privacy Program. The Contractor must 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. The Contractor's Privacy Program must 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. The Contractor's Privacy Policies, guidelines, and procedures must 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. The Contractor's Privacy Program must include performing ongoing monitoring and audits of operations to identify and mitigate privacy Threats.

The Contractor must exercise the same degree of care in safeguarding and protecting County information that the Contractor exercises with respect to its own information and data and, at a minimum, a reasonable degree of care. The Contractor will implement, maintain, and use appropriate privacy practices and protocols to preserve the Confidentiality of County Information.

The Contractor's Privacy Program must include:

- A Privacy Program framework that identifies and ensures that the 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 must not be used by the 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 the Contractor, or commercially exploited or otherwise used by, or on behalf of, the Contractor, its officers, directors, employees, or agents. The 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, the 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 the 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. The Contractor specifically consents to the County's access to such County Information held, stored, or maintained on any and all devices Contactor owns, leases or possesses.

4. CONTRACTOR'S USE OF COUNTY INFORMATION

The Contractor may use County Information only as necessary to carry out its obligations under the Contract. The Contractor must 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 State and federal law governing the protection of personal Information, (ii) any 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

The Contractor must 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. The Contractor agrees that all County Information is confidential and proprietary to the County regardless of whether such information was disclosed intentionally or unintentionally or marked as "confidential". All County Information received by the Contractor must be marked in writing as "Confidential". Notwithstanding the foregoing, failure to mark any document containing Confidential Information as "Confidential" prior to disclosure will not exempt it from confidential treatment.

b. Disclosure of County Information. The 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 the County's Contract administrator in consultation with the 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, the Contractor must notify the County's Contract administrator 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, the Contractor may encounter County non-public information ("NPI"), 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. The Contractor must not disclose or publish any County NPI and/or material received or used in performance of the Contract. This obligation is perpetual.

d. Individual Requests. The Contractor must acknowledge any request or instruction from the County regarding the exercise of any individual's privacy rights provided under applicable federal or State laws. The Contractor must 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 calendar days. If an individual makes a request directly to the Contractor involving County Information, the Contractor must notify the County within five calendar days and the County will coordinate an appropriate response, which may include instructing the Contractor to assist in fulfilling the request. Similarly, if the Contractor receives a privacy or security complaint from an individual regarding County Information, the Contractor must notify the County as described in Section 14 below, SECURITY AND PRIVACY INCIDENTS, and the County will coordinate an appropriate response.

e. Retention of County Information. The Contractor must not retain any County Information for any period longer than necessary for the Contractor to fulfill its obligations under the Contract and applicable law, whichever is longest.

7. CONTRACTOR EMPLOYEES

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

The Contractor must supply each of its employees with appropriate annual training regarding Information Security procedures, Risks, and Threats. The 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:** The Contractor's Privacy Policies and procedures as described in Section 2b above, Privacy Program.

The Contractor must have an established set of procedures to ensure the 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, the 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 Attachment will also apply to all Subcontractors and third parties. The 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 Attachment, both for itself and to enable the 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 Attachment; and (ii) the 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 the Contract.

The Contractor must obtain advanced approval from the County's Chief Information Security Officer and/or Chief Privacy Officer prior to subcontracting services subject to this Attachment.

9. STORAGE AND TRANSMISSION OF COUNTY INFORMATION

All County information should be protected via encryption whether at rest or during transport so as to prevent unauthorized individuals the ability to read, use or decipher said information. The Contractor will encrypt all workstations, portable devices (such as mobile, wearables, and tablets), removable media (such as portable or removable hard disks, floppy disks, USB memory drives, CDs, DVDs, magnetic tape, and all other removable storage media), servers (whether virtual or physical) and/or systems (including Cloud platforms, infrastructure and services) that store County Information in accordance with Federal Information Processing Standard (FIPS) 140-2 or otherwise approved by DMH's Information Security Officer.

The Contractor will encrypt County Information transmitted on networks outside of the Contractor's control with the latest or 1 version removed from latest, Transport Layer Security (TLS) or Internet Protocol Security (IPSec), which uses a minimum cipher strength of 128 bit or higher. Contractor must request and be granted approval by DMH's Information Security Officer in order to use an alternative or equivalent secure transmission protocol or method.

In addition, the Contractor must request and be granted approval by DMH's Information Security Officer in order to store County Information on any cloud infrastructure, platform service or in any other online storage provider.

All mobile devices storing County Information must 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 the DMH's Information Security Officer.

10. RETURN OR DESTRUCTION OF COUNTY INFORMATION

The Contractor must 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 County's written request, or upon expiration or termination of the Contract for any reason, Contractor must (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 the 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, the Contractor must 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, the Contractor must provide an attestation on company letterhead and certified documentation from a media destruction firm consistent with subdivision b of this Section. Upon termination or expiration of the Contract or at any time upon the County's request, the Contractor must return all hardware, if any, provided by the County to the Contractor. The hardware should be physically sealed and returned via a bonded courier, or as otherwise directed by the County.

b. Method of Destruction. The Contractor must 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 the County Information cannot be retrieved. The Contractor will provide an attestation on company letterhead and certified documentation from a media destruction firm, detailing the destruction method used and the 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 contract manager within 10 days of termination or expiration of the Contract or at any time upon the County's request. On termination or expiration of this Contract, the County will return or destroy all Contractor's Information marked as confidential (excluding items licensed to the County hereunder, or that provided to the County by the 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

The Contractor must: (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 below, SECURITY AND PRIVACY INCIDENTS; (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.

The 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 the Contractor makes backups to removable media (as described in Section 9 above, STORAGE AND TRANSMISSION OF COUNTY INFORMATION), all such backups must 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 above, 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 the County Project Director or Project Manager in writing; and (ii) if transferred using removable media (as described in Section 9 above, STORAGE AND TRANSMISSION OF COUNTY INFORMATION) must be sent via a bonded courier and protected using encryption technology designated by the Contractor and approved by the County's Chief Information Security Officer in writing. The foregoing requirements will apply to back-up media stored by the Contractor at off-site facilities.

The Contractor must 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 must 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. The 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. The Contractor must record, review and act upon all events in accordance with Incident response policies set forth in Section 14 below, SECURITY AND PRIVACY INCIDENTS; and

f. In the event any hardware, storage media, or removable media (as described in Section 9 above, STORAGE AND TRANSMISSION OF COUNTY INFORMATION) must be disposed of or sent off-site for servicing, the Contractor must ensure all County Information has been eradicated from such hardware and/or media using industry best practices as discussed in Section 9 above, STORAGE AND TRANSMISSION OF COUNTY INFORMATION.

14. SECURITY AND PRIVACY INCIDENTS

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

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

Chief Information Security Officer:
Jeffrey Aguilar
Chief Information Security Officer
320 W Temple, 7th Floor
Los Angeles, CA 90012
Phone: (213) 253-5659

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

County Chief Information Security Officer and Chief Privacy Officer email
CISO-CPO_Notify@lacounty.gov

DMH Departmental Information Security Officer:
DMH Departmental Information Security Officer
510 S. Vermont Avenue, 16th Floor
Los Angeles, CA 90020
Phone: (213) 651-7224
DMH Departmental Information Security Officer email:
InformationSecurity@dmh.lacounty.gov

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 organization's 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 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 the Contractor, and unless prohibited by law, the Contractor must provide Information regarding the nature and consequences of the Incident that are reasonably requested by the County.

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 the Contractor's environment that may include, but are not limited to, interviews of relevant employees, reviews of documentation, or technical inspections 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/or this Attachment, the 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 the Contractor's weaknesses, negligence, errors, or lack of Information Security or privacy controls or provisions.

15. NON-EXCLUSIVE EQUITABLE REMEDY

The 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 above, CONFIDENTIALITY, will constitute a material breach of the Contract and

be grounds for immediate termination of the Contract in the exclusive discretion of the County.

16. AUDIT AND INSPECTION

a. Self-Audits. The Contractor must 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 the County.

The Contractor must have a process for correcting control deficiencies that have been identified in the periodic audit, including follow up documentation providing evidence of such corrections. The Contractor must provide the audit results and any corrective action documentation to the County promptly upon audit completion, at the County's request. With respect to any other report, certification, or audit or test results prepared or received by the Contractor that contains any County Information, the Contractor must promptly provide the County with copies of the same upon the County's reasonable request, including identification of any failure or exception in the Contractor's Information systems, products, and services, and the corresponding steps taken by the Contractor to mitigate such failure or exception. Any reports and related materials provided to the County pursuant to this Section must 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 the 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, the Contractor must 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 the Contractor has materially breached this Attachment, in which case the Contractor will bear all costs of the audit; and if the audit reveals material non-compliance with this Attachment, the County may exercise its termination rights under the Contract.

Such audit will be conducted during the Contractor's normal business hours with reasonable advance notice, in a manner that does not materially disrupt or otherwise unreasonably and adversely affect the 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. The Contractor must 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. The Contractor agrees to comply with all reasonable recommendations that result from such inspections, tests, and audits within reasonable timeframes.

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

c. Federally Mandated Audits, The Health Information Technology for Economic and Clinical Health (HITECH) Act requires the Office Of Civil Rights (OCR) within the Department of Health and Human Services (HHS) to periodically audit covered entities and business associates for their compliance with the HIPAA Privacy, Security, and Breach Notification Rules. The Contractor will promptly notify the County of any OCR audit or investigation and will keep the County informed of the progress and results of such audit or investigation. The Contractor will also provide the County with copies of any reports, findings, or recommendations issued by the OCR as a result of the audit or investigation.

17. CYBER LIABILITY INSURANCE

The Contractor must 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.

The Contractor must secure and maintain cyber liability insurance coverage with limits of at least $2 million 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. The Contractor must add the County as an additional insured to its cyber liability insurance policy and provide to the 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, must not be construed as a limitation upon the 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, the 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 :

- The Contractor's violation of any federal and State laws in connection with its accessing, collecting, processing, storing, disclosing, or otherwise using County Information;

- The Contractor's failure to perform or comply with any terms and conditions of the Contract or related agreements with the County; and/or,

- Any Information loss, breach of Confidentiality, or Incident involving any County Information that occurs on the Contractor's systems or networks (including all costs and expenses incurred by the 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 County with a full and adequate defense, as determined by County in its sole judgment, County will be entitled to retain its own counsel, including, without limitation, County Counsel, and County will be entitled to reimbursement from Contractor for all such costs and expenses incurred by 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 County without County's prior written approval.

19. CERTIFICATION

Within 10 business days of the receipt of this document, Contractor must complete and provide to County the Attachment 2 of Exhibit K "DMH Contractor's Compliance with Information Security Requirements" questionnaire (for itself and on behalf of its subcontractors) certifying that will be compliant with Los Angeles County Board of Supervisors' Policies and attest that it has implemented adequate controls to meet the expected Information Security minimum standard set forth above, at the commencement and during the term of the Contract.

In addition, Contractor must be prepared to provide supporting evidence upon request to validate its compliance. Failure on the part of the Contractor to comply with any of the provisions of this Attachment, "Information Security and Privacy

Requirements for Contracts" will constitute a material breach of this arrangement upon which the County may terminate or suspend the Contract.

20. REPORTING REQUIREMENTS FOR SIGNIFICANT CHANGES

During the term of the Contract, Contractor must notify the County within 10 days of implementation, in writing, about any significant changes such as technology changes, modification in the implemented security safeguards or any major infrastructure changes. Depending on the change(s), Contractor may be asked to re-submit Attachment 2 of Exhibit K, "DMH Contractor's Compliance with Information Security Requirements".

21. MAINTAINING COMPLIANCE

Contractor must provide updates about its information security practices **annually** by completing Attachment 2 of Exhibit K, "DMH Contractor's Compliance with Information Security Requirements" questionnaire. By submitting, Contractor certifies that its implemented controls will continue to be in compliance with Los Angeles County Board of Supervisors' Policies, and the expected minimum standard set forth above during the term of any arrangement that may be awarded pursuant to this agreement. The completed forms must be returned to DMH Information Security Officer (DISO) within 10 business days of receipt and must be approved for continuous business with the County.

ADDENDUM A: SOFTWARE AS A SERVICE (SaaS)

a. License: Subject to the terms and conditions set forth in the Contract, including payment of the license fees to the Contractor, the Contractor hereby grants to County a non-exclusive, non-transferable worldwide County license to use the SaaS, as well as any documentation and training materials, during the term of the Contract to enable the County to use the full benefits of the SaaS and achieve the purposes stated therein.

b. Business Continuity: In the event that the Contractor's infrastructure containing or processing County Information becomes lost, altered, damaged, interrupted, destroyed, or otherwise limited in functionality in a way that affects the County's use of the SaaS, the Contractor must immediately and within 24 hours, implement the Contractor's Business Continuity Plan, consistent with Section 12 of this Attachment, OPERATIONAL MANAGEMENT, BUSINESS CONTINUITY, AND DISASTER RECOVERY, such that the Contractor can continue to provide full functionality of the SaaS as described in the Contract.

The Contractor will indemnify the County for any claims, losses, or damages arising out of the County's inability to use the SaaS consistent with the Contract and Section 18 of this Attachment , PRIVACY AND SECURITY INDEMNIFICATION.

The Contractor must include in its Business Continuity Plan service offering, a means for segmenting and distributing IT infrastructure, disaster recovery and mirrored critical system, among any other measures reasonably necessary to ensure business continuity and provision of the SaaS.

In the event that the SaaS is interrupted, the County Information may be accessed and retrieved within two hours at any point in time. To the extent the Contractor hosts County Information related to the SaaS, the Contractor must create daily backups of all County Information related to the County's use of the SaaS in a segmented or off-site "hardened" environment in a manner that ensures backups are secure consistent with cybersecurity requirements described in this Contract and available when needed.

c. Enhancements: Upgrades, replacements and new versions: The Contractor agrees to provide to County, at no cost, prior to, and during installation and implementation of the SaaS any software/firmware enhancements, upgrades, and replacements which the Contractor initiates or generates that are within the scope of the SaaS and that are made available at no charge to the Contractor's other customers.

During the term of the Contract, the Contractor must promptly notify the County of any available updates, enhancements or newer versions of the SaaS and within 30 days update or provide the new version to the County. The Contractor must provide any accompanying

documentation in the form of new or revised documentation necessary to enable the County to understand and use the enhanced, updated, or replaced SaaS.

During the Contract term, the Contractor must not delete or disable a feature or functionality of the SaaS unless the Contractor provides 60 days' advance notice and the County provides written consent to delete or disable the feature or functionality. Should there be a replacement feature or functionality, the County will have the sole discretion whether to accept such replacement. The replacement will be at no additional cost to the County. If the Contractor fails to abide by the obligations in this section, the County reserves the right to terminate the Contract for material breach and receive a pro-rated refund.

d. Location of County Information: The Contractor warrants and represents that it will store and process County Information only in the continental United States and that at no time will County Data traverse the borders of the continental United States in an unencrypted manner.

e. Annual Data Center Audit and Certification: The Contractor agrees to conduct an annual System and Organization Controls (SOC 2 type II) audit or equivalent (i.e. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27001:2013 certification audit or Health Information Trust Alliance (HITRUST) Common Security Framework certification audit) of its internal controls for security, availability, integrity, confidentiality, and privacy. The Contractor must have a process for correcting control deficiencies that have been identified in the audit, including follow up documentation providing evidence of such corrections. The results of the audit and the Contractor's plan for addressing or resolving the audit findings must be shared with County's Chief Information Security Officer within 10 business days of the Contractor's receipt of the audit results. The Contractor agrees to provide County with the current audit certifications upon request.

f. Services Provided by a Subcontractor: At least 30 days prior to engaging a Subcontractor for the SaaS under the Contract, the Contractor must notify County of the proposed subcontractor(s) and the purposes for which they may be engaged and obtain written consent of the County's Contract Administrator.

g. Information Import Requirements at Termination: Within one day of notification of termination of the Contract, the Contractor must provide County with a complete, portable, and secure copy of all County Information, including all schema and transformation definitions and/or delimited text files with documented, detailed schema definitions along with attachments in a format to be determined by County upon termination.

h. Termination Assistance Services: During the 90 day period prior to, and/or following the expiration or termination of the Contract, in whole or in part, the Contractor agrees to provide reasonable termination assistance services at no additional cost to County, which may include:

(i) Developing a plan for the orderly transition of the terminated or expired SaaS from the Contractor to a successor;

(ii) Providing reasonable training to County staff or a successor in the performance of the SaaS being performed by the Contractor;

(iii) Using its best efforts to assist and make available to the County any third-party services then being used by the Contractor in connection with the SaaS; and

(iv) Such other activities upon which the Parties may reasonably agree.

ADDENDUM B: CONTRACTOR HARDWARE CONNECTING TO COUNTY SYSTEMS

Notwithstanding any other provisions in the Contract, the Contractor must ensure the following provisions and security controls are established for any and all Systems or Hardware provided under the Contract.

a. Inventory: The Contractor must actively manage, including through inventory, tracking, loss prevention, replacement, updating, and correcting, all hardware devices covered under the Contract. The Contractor must be able to provide such management records to the County at inception of the Contract and upon request thereafter.

b. Access Control: The 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, the Contractor must document its 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 the County's Chief Information Security Officer (CISO) for review and approval. The Contractor must modify and/or implement such plan as directed by the DISO and CISO.

c. Operating System and Equipment Hygiene: The 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. The Contractor agrees to ensure that the operating system is configured to eliminate any unnecessary applications, services and programs. If for some reason the Contractor cannot do so within 90 days, the Contractor must provide a Risk assessment to the County's CISO.

d. Vulnerability Management: The Contractor agrees to continuously acquire, assess, and take action to identify and remediate vulnerabilities within the Systems and Hardware covered under this Contract. If such vulnerabilities cannot be addressed, The Contractor must provide a Risk assessment to the DISO who will consult with the CISO. The County's CISO must approve the Risk acceptance and the 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, the 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 the County's CISO.

f. Malware Protection: The Contractor will provide and maintain industry-standard endpoint antivirus and antimalware protection on all Systems and Hardware as approved or required by the DISO who will consult with the County's CISO to ensure provided hardware is free and remains free of malware. The Contractor agrees to provide the County documentation proving malware protection status upon request.

ADDENDUM C: APPLICATION SOURCE CODE REPOSITORY

The Contractor must 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 the Contract, (hereinafter referred to as "County Source Code") must 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.