INFORMATION SECURITY AND PRIVACY

County's Information Assets are essential to the continued operation of the County and Department and must be protected in a manner commensurate with its sensitivity, value, and criticality. It is the responsibility of the Contractor to adhere and implement the required measures and safeguards to protect and preserve the privacy, confidentiality, availability and integrity of County Confidential Information (electronic and hard copy and in any form, format or medium, in-transit and at-rest) from unauthorized disclosure, modification, or destruction, and shall safeguard them to the extent permitted by law.

Information Security and Privacy provisions and requirements extends to all subcontractors, agents, individuals, entities, and/or organization operating on behalf of the Contractor that handle (e.g., access, view, transport, transmit, store) County Information Assets to perform work under this Agreement.

Confidential Information: County requires its contractors, subcontractors, and agents to keep confidential all data, records and information (electronic and hard copy, in-transit and at-rest, and in any form, format or medium) which are designated or marked as Confidential Information as prescribed herein. The parties agree, to implement proper and sufficient administrative, technical, and physical safeguards to protect Confidential Information, and comply with legal and County mandates as applicable. Confidential Information includes information which is exempt from public disclosure in specific legislation or which is identified as personal, sensitive, or confidential such as personally identifiable information (PII), individually identifiable health information (PHI), medical records (MI), employment and education records, and non-public information as specified in all applicable federal, State and local laws and regulations. In general, any data and information that is exempt from public disclosure under either federal, State, local laws and County policies is confidential. If the receiving party is required to produce the data by law, court order, or governmental authority, the disclosing party must be promptly notified of such obligation.

The parties shall: (a) use Confidential Information, as set forth in this Contract and otherwise for the purposes or projects approved by the County; (b) ensure individual anonymity and adhere to the mandates for confidentiality; (c) not disclose or disseminate any Confidential Information including Personally Identifiable Information (PII), Protected Health Information (PHI) and Medical Information (MI) to the public; (d) implement reasonable and adequate measures and safeguards to protect and preserve the privacy, confidentiality, availability and integrity of County Confidential Information (electronic and hard copy); and (e) implement reasonable and necessary measures to timely identify, detect, protect, respond, mitigate, and prevent against any (intentional or accidental) unauthorized acquisition, access, use, modification, disclosure, loss or damage of County Confidential Information by any cause (manmade and natural); and (f) Comply, as applicable, with federal, State, local, and County data and information protection rules, laws, regulations, mandates, ordinances, standards, best practices, guidelines, directives, policies and procedures including but not limited to the California Public Records Act, First Amendment, privacy laws, the California Education Code, California Information Practices Act of 1977, the Federal Privacy Act of 1974, and the Federal

Family Education Rights and Privacy Act of 1974, California Civil Code Section 1798.82, California Penal Code Section 502, Health Insurance Portability and Accountability Act of 1996 (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), and Los Angeles County Board of Supervisors Policy Manual Chapters 3 (3.040 - Records Management and Archive of County Records), 5 (5.200 - Contractor Protection of Electronic County Information) and 6 of County's Policy Manual, which can be accessed at https://library.municode.com/ca/la_county_-_bos/codes/board_policy?nodeId=CH6INTE.

During the course of this Contract, the parties may provide each other with certain information, data, or materials in writing which the disclosing party has clearly marked or identified in writing as confidential or proprietary in nature or if orally disclosed, reduced to writing by disclosing party within thirty (30) days of disclosure ("Confidential Information"). The receiving party shall receive and hold Confidential Information in confidence and agrees to use its reasonable efforts to prevent disclosure to third parties of Confidential Information in the manner the receiving party treats its own similar information, but in no case less than reasonable care shall be exercised by the receiving party. Except as required by law or with permission from disclosing party, receiving party will not disclose Confidential Information.

The parties shall, as needed, inform all of its officers, employees, and agents engaged in the performance of this Contract of the confidentiality provisions of this Contract. Contractor shall have in place with its officers, employees and agents including subcontractors written agreements having the effect of requiring such individuals to protect and keep Confidential Information confidential and protected.

DATA HOSTING SECURITY

Contractor shall comply with the current Cloud Security Alliance's (CSA) Cloud Control Matrix (CCM) security requirements for Contractor hosted services or applications that are included as part of Contractor's solution (https://cloudsecurityalliance.org/research/ccm/), and adhere to The National Institute of Standards and Technology (NIST), and/or Information Security Management System Standards 27001 and 27002 promulgated by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), as such Standards relate to risk assessment, training and awareness, metrics and reporting, organization and allocation of responsibilities, incident management, and compliance.

ACCESS

Contractor shall implement multi-layered adequate administrative, technical, and physical access control mechanisms and authentication and authorization verification process while enforcing separation of duties on systems and infrastructure handling County data and information, including but not limited to, Multifactor Authentication (MFA) and to constantly monitor, protect, and limit the use and disclosure of information to minimum necessary required to accomplish the purposes described in this Agreement. Access to County data must follow the principle of least privilege and limited to those personnel with a legitimate business justification on need-to-know basis required to perform work under

this Agreement. Access to County data and information shall immediately suspend, terminated, or removed upon business need is fulfilled, upon suspension or termination of employment, contract, or agreement.

SYSTEM ACQUISITION, DEVELOPMENT, AND MAINTENANCE
Contractor shall adopt and implement adequate security and privacy measure (administrative, technical and physical) and provisions and use industry accepted standard and framework for purchase, use, or development of information systems, including application services delivered through public networks. Such measures include but not limited to use of Web Application Firewall (WAF) for all application and system that process County data and information.

VULNERABILITY ASSESSMENT
Contractor shall perform an adequate and comprehensive vulnerability assessment and address all findings prior to final delivery of the product to the County.

AUDIT TRAILS AND LOGGING
The system/application shall chronologically record, log, store and adequately retain all system events, transact ions, and user activities and actions consistent with NIST SP 800-92 Guide to Computer Security Log Management (https://csrc.nist.gov/publications/detail/sp/800-92/final). At minimum, logs shall include but not limited to, the following:

1. Successful and failed application authentication attempts;
2. Date and time;
3. User or system account associated with an event;
4. Device used (e.g. source and destination IPs, terminal session ID, web browser, etc.)
5. Operating System type and version;
6. log on attempts (successful or unsuccessful);
7. Function(s) performed after logged on;
8. Configuration changes;
9. Account changes (e.g., account creation and deletion, account privilege assignment);
10. Successful/failed; and
11. Use of privileged accounts.

CRYPTOGRAPHY

a. **STORAGE OF DATA**
Contractor shall adequately secure and encrypt all County's electronic data and information while at storage (e.g., servers, workstations, portable/mobile devices, wearables, tablets, thumb drives, external hard drives, etc.) using Advanced Encryption Standard (AES) with a minimum cipher strength of 256-bit in accordance with: (a) Federal Information Processing Standard Publication (FIPS) 140-2; (b)

National Institute of Standards and Technology (NIST) Special Publication 800-57 Recommendation for Key Management – Part 1: General (Revision 3); (c) NIST Special Publication 800-57 Recommendation for Key Management – Part 2: Best Practices for Key Management Organization; and (d) NIST Special Publication 800-111 Guide to Storage Encryption Technologies for End User Devices.

b. TRANSFER OF DATA

Data and information shall be transferred and transmitted security via online methods such as secure file transfer (SFTP) software, encrypted email or using encrypted magnetic or optical media. The Parties shall determine the transfer method appropriate for the Project. All transmitted data and information must be encrypted using the latest stable version of Secure Sockets Layer (SSL)/Transport Layer Security (TLS) with a minimum cipher strength of 128-bit in accordance with: (a) NIST Special Publication 800-52 Guidelines for the Selection and Use of Transport Layer Security Implementations; and (b) NIST Special Publication 800-57 Recommendation for Key Management – Part 3: Application–Specific Key Management Guidance.

RETURN OF DATA

Upon termination of this Agreement, Contractor must return or thoroughly and irretrievably destroy all County data and information in any form, format or medium. County data and information (electric and hard copy) must be properly purged, cleared, shredded, sanitized or destroyed in fashion that it is rendered unusable, unreadable, or indecipherable to unauthorized individuals consistent with National Institute of Standards and Technology (NIST) Special Publication 800-88, Guidelines for Media Sanitization. Contractor shall provide proper and satisfactory proof of proper destruction and sanitization of County data and information within ten (10) business days of data destruction.

CERTIFICATION

County must receive within ten (10) business days of its request, a certification from Contractor (for itself and any Sub-Contractors) that certifies and validates compliance with the encryption standards set forth above. In addition, Contractor shall maintain a copy of any validation/attestation reports that its data encryption product(s) generate, and such reports shall be subject to audit in accordance with the Contract. Failure on the part of the Contractor to comply with any of the provisions shall constitute a material breach of this Contract upon which the County may terminate or suspend this Contract.

DISCLOSURE OF SECURITY INCIDENT AND DATA BREACH

The Contractor shall notify the County no later than (48) hours or two business days upon discovery or reasonable belief of any suspected, attempted, successful, or imminent threat of unauthorized electronic or physical access, use, modification, exposure, acquisition, disclosure, compromise, breach, loss or destruction of County data and information; interference with Information Technology operations; or significant violation of County or departmental policy (“Security Incident”). Breach reports of shall include, to the extent available, the identification of each individual whose Data has been, or is reasonably believed to have been accessed, viewed, acquired, or disclosed during such

breach. Security incidents that do not result in any unauthorized access, use, disclosure, modification, destruction of information or interference with system operations may be reported in the aggregate upon written request of County in a manner and frequency mutually acceptable to the Parties. The Parties acknowledge that incidents including, but not limited to, ping sweeps or other common network reconnaissance techniques, attempts to log on to a system with an invalid password or username, and denial of service attacks that do not result in a server being taken off line, may occur from time to time.

AGREEMENT TO OBEY ALL LAWS

The Parties shall at all times observe, comply with, and perform all obligations hereunder in accordance with all applicable federal, state, county, and local governmental agencies laws, ordinances, codes and regulations that in any manner affect the terms of this Agreement.

CYBER INSURANCE REQUIREMENT

As applicable, contractor will maintain sufficient cyber insurance to cover any and all losses, security breaches, privacy breaches, unauthorized distributions, or releases or uses of any data transferred to or accessed by Contractor under or as a result of this Contract. This insurance shall provide sufficient coverage(s) for the Contractor, the County, and affected third parties for the review, repair, notification, remediation and other response to such events, including but not limited to, breaches or similar incidents. The Contractor shall obtain modified coverage(s) as reasonably requested by the County within ten (10) business days of the Contractor's receipt of such request from the County.

Notice to COUNTY related to information security shall be forwarded to COUNTY and also to the DCFS Chief Information Security Officer:

Allen Ohanian
Department of Children and Family Services
Chief Information Security Officer
12440 Imperial Hwy
Norwalk, California 90650
Telephone: (323) 627-9855
Email: aohanian@dcfs.lacounty.gov