NON-IT SERVICES CONTRACTS CONFIDENTIALITY AND DATA SAFEGUARDS

OPTIONAL SPECIAL PROVISIONS TO SELECT FROM FOR INCLUSION IN CONTRACTS INVOLVING USE OF CONFIDENTIAL STATE DATA

1. DEFINITIONS:
    1.1. **Confidential Information** means any non-public information, whether in written, oral, graphic, electronic or any other form, including and without limitation, unpublished financial information, state plans and practices, and projections, and marketing data, business, financial, technical information, user manuals, forecasts, analyses, software and processes, or information which would be deemed by a reasonable person to be confidential or proprietary in nature. Confidential Information also means an individual's health, genetic or biometric information, race, ethnic origin, sexual orientation, religious or political, beliefs/affiliation, or criminal record. The contracting state agency may also designate information as "Confidential" or "Proprietary."
    1.2. **Personal Information** as set forth in Civil Code section 1798.3, subdivision (a) of the California Information Practices Act (§1798 et. seq) means any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, their name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual.
    1.3. **State Data** means all information and data owned by the State and submitted to, processed by, or stored by the Contractor and includes, but is not limited to, all data/information that originated with the State, all data/information provided by the State, and data/information generated, manipulated, produced, reported by or otherwise emanating from or by applications run by the State. State Data encompasses Confidential Information and Personal Information.
    1.4. **Security Incident** means any actual or suspected unauthorized access, destruction, loss, theft, use, modification, or disclosure of State Data.

2. DATA PRIVACY AND CONFIDENTIALITY:
    2.1. Contractor shall not collect, use, retain, disclose, sell or otherwise make use of State Data for Contractor's own commercial purposes or in a way that does not comply with the purpose of this Contract or applicable law. Contractor shall notify the State by the fastest means available, not later than 48 hours after receipt, of any subpoena, warrant, court order, service of process, California Public Records Act (Gov. Code, § 7920.00 et seq.) request, and or other legal request ("Requests") which seeks access to State Data, unless such notification is prohibited by law. Unless prohibited by law, Contractor shall also provide written notice to Contracting agency (Buyer) and to the Agency Chief Information Security Officer (CISO) or designee of Contracting agency. Unless prohibited by law, Contractor shall not respond to such Requests unless authorized in writing to do so by the State and shall not respond to such Requests directed at Contractor regarding the Contract without first notifying the State in writing. Unless prohibited by law, Contractor

shall provide the State with its intended responses to such Requests with adequate time for the State to review, revise, and, if necessary, seek a protective order.

2.2. Contractor shall ensure confidentiality and security of State Data. Contractor shall ensure that all its personnel as well as personnel of its subcontractors with access to State Data comply with security and confidentiality obligations set forth in the Contract.

2.3. Contractor will not disclose State Data or allow access to such information to any third party without the State's prior written consent; provided, however, that Contractor may disclose State Data to its affiliates and subcontractors for purposes of providing the services to the State under this Contract. Contractor will be liable for all actions by the subcontractor related to the use, processing and/or disclosure of State Data.

2.4. Contractor will return or render permanently unreadable and unrecoverable all State Data at the end of this Contract or upon the State's written request unless State Data must be retained by Contractor to comply with applicable laws. Erasure or destruction of all State Data in Contractor's possession shall be in accordance with State's standard for data destruction, which State shall provide to Contractor. Contractor shall provide certification of destruction to State.

3. DATA PROTECTION:

3.1. *Safeguards*. Contractor shall implement and maintain all appropriate administrative, physical, technical, and procedural safeguards in accordance with applicable laws, policies, and regulations at all times during the Contract term to protect State Data, systems, and services, from unauthorized or unlawful use, access, modification, disclosure or destruction, introduction of viruses, disabling devices, malware and other forms of malicious or inadvertent acts.

3.2. *Security Incident*. Unless otherwise specified in the Contract or Statement of Work, upon discovery or reasonable belief of any Security Incident, Contractor shall notify the State in writing by the fastest means available, in no event greater than 48 hours after such discovery or belief.

3.2.1. Contractor's notification shall identify, to the full extent known to Contractor:

3.2.1.1. The nature of the Security Incident;

3.2.1.2. The State Data improperly accessed, used, or disclosed;

3.2.1.3. The individual records improperly accessed, used, or disclosed if Confidential Information or Personal Information is involved;

3.2.1.4. The person(s) who improperly accessed, used, disclosed or received State Data;

3.2.1.5. What Contractor has done or will do to quarantine and remediate the Security Incident; and

3.2.1.6. What corrective action(s) Contractor has taken or will take to prevent future Security Incidents.

3.2.2. Contractor shall take prompt corrective action to mitigate any risks or damages involved with the Security Incident.

3.2.3. If Contractor experiences a Security Incident, the State shall determine whether notification to any individuals whose State Data has been improperly accessed, lost or breached is appropriate. If Confidential Information or Personal Information is reasonably believed to have been improperly accessed or acquired by an unauthorized person as a result of a Security Incident that is not due to the fault of the State or any person or entity under the control of the State, Contractor shall bear any and all costs associated with the State's notification obligations as required by all applicable laws and regulations, as well as the cost of credit monitoring. Contractor shall immediately investigate the Security Incident and shall share the investigation report with the State. The State or its authorized agents reserve the right to lead (if required by law) or participate in the investigation. Contractor shall cooperate fully with the State, its agents, and law enforcement.

3.2.4. If the State determines that the data loss or Security Incident is significant, at the discretion of the State, Contractor will, at its expense, have an independent, industry-recognized, State-approved third party perform an information security audit. Contractor shall immediately share the audit results with the State upon Contractor's receipt of such results. Contractor will provide the State with written evidence of planned remediation within thirty (30) days from receipt of the audit results and promptly modify its security measures.

4. SURVIVAL:
These privacy, confidentiality, and protection obligations of Contractor, its, agents, successors, and/or assigns, continues for so long as Contractor has access to State Data, including required retention or storage timeframes after Contract termination or expiration.