INFORMATION SECURITY AND PRIVACY PROVISIONS DATED 2/2021

In the performance of this Contract, [Contractor] agrees to protect all Department of Motor Vehicles (DMV) information by implementing the necessary controls to comply with State mandated security and privacy requirements provided in California State Administrative Manual (SAM), National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS), Government Code §11015.5 and §11019.9, Vehicle Code, and California Information Practices Act (IPA) Civil Code §1978 et seq. The Contractor further agrees to implement the minimum administrative, physical, technical, and safeguards identified in this Contract. The Contractor shall protect DMV information for the terms and length of this Contract and while in possession of, maintaining, or accessing DMV information. The Contractor shall ensure any third parties adhere to these same provisions.

A. DEFINITIONS

For purposes of this Exhibit, the following definitions shall apply:

1. **Contractor** shall generally refer to any entity, private or public organization hired or working in conjunction with or for DMV to provide deliverables.
2. **Data** shall mean a representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automated means.
3. **DMV Information** shall refer to DMV provided data.
4. **Confidential information** shall have the same meaning as those terms in SAM, IPA, Civil Codes, and related Government Codes.
5. **Personal information** shall have the same meaning as those terms in SAM, IPA, Civil Codes, and related Government Codes.
6. **Sensitive information** shall have the same meaning as those terms in SAM, IPA, Civil Codes, and related Government Codes.
7. **Personnel** shall refer to any Contractor employees, volunteers, contractors, sub-contractors commissioned, employed by, or otherwise engaged in the performance of work associated with the Contractor.
8. **Systems** shall refer to workstations, laptops, servers, network, and other information processing components
9. **Users** shall refer to any Contractor personnel with access to DMV information.

B. ADMINISTRATIVE SAFEGUARDS

1. DATA OWNERSHIP

DMV information provided under this Contract remains DMV exclusive property. Confidential, sensitive, and personal information is not open to the public and requires special precautions to protect from loss and unauthorized use, disclosure, modification, or destruction. This information must not be shared without written permission from the DMV.

The Contractor recognizes its responsibility to protect the confidentiality of information in their custody as provided by law and ensure such information is disclosed only to those individuals, and of such purpose as authorized by the respective laws.

The Contractor shall have a non-exclusive right to use and process the disclosed information for the purposes stated in this Contract. This right shall be revoked immediately upon termination of this Contract. Disclosure of this data does not transfer ownership of information to the Contractor.

2. USE OF INFORMATION

The Contractor acknowledges and agrees that the information furnished or secured pursuant to this Contract shall be used solely for the purposes described in this Contract, and agrees to implement policies and procedures to ensure the confidentiality of said information.

The Contractor further agrees that information obtained under this Contract shall not be reproduced, published, sold, or released in original or any other form for any purpose other than identified in this Contract. Only the minimum necessary amount of DMV information required to perform necessary business functions may be processed, stored, or transmitted.

The Contractor shall not use any DMV information that identifies real individuals for any purpose not described in this Contract, including for testing, training, or research.

3. BACKGROUND CHECKS

Contractor Personnel who may access DMV information, must undergo a thorough background check, with evaluation of the results to assure that there is no indication that the worker may present a risk to the security or integrity of confidential data or a risk for theft or misuse of confidential data. The Contractor shall retain background check documentation for a period of three (3) years following contract termination.

4. STATEMENT OF CONFIDENTIALITY AND REQUIREMENTS

Information maintained by DMV is confidential under this Contract and exempt from disclosure under the provisions of California Public Records Act (Government Code §6250-6265), the California Elections Code §2194), and other applicable state or federal laws.

The Contractor further understands and acknowledges that under California Penal Code §502, it is a public offense to knowingly and without permission alter, damage, delete, destroy, copy, or otherwise use any DMV data. Such action can be prosecuted civilly or criminally, and is punishable by fine and/or imprisonment.

The Contractor shall ensure that all users sign a confidentiality statement each year, attesting to the fact that he/she is aware of the confidential nature of the data and penalties for unauthorized disclosure under applicable state and federal law. Copies of signed confidentiality statements must be made available to the DMV CISO upon request.

5. INFORMATION SECURITY AND PRIVACY AWARENESS TRAINING

The Contractor shall ensure that all users must receive information security and privacy awareness training prior to accessing such information, and annually thereafter. Information security and privacy awareness training must contain instructional components such as, but not limited to, information about the confidential nature of information, laws and regulations protecting the confidentiality of information, user responsibility for protecting the information, and the consequences and legal liability of unauthorized use, access, or disclosure of said information. Upon request, the Contractor must provide the DMV Chief Information Security Officer (CISO) or Privacy Officer with a copy of its information security and privacy awareness training components and certification of its annual information security and privacy awareness training completion.

6. EMPLOYEE ACCESS TO INFORMATION

The Contractor agrees that information shall be kept in the strictest confidence and only made available to authorized personnel on a "need-to-know" business basis, and only for the purposes authorized under this Contract. The term "need-to-know" refers to those authorized persons who need information to perform their official duties in connection with the purpose described in the Contract.

The Contractor shall maintain records of all authorized users and the authorization level of access granted to the information obtained under this Contract with the purpose described in this Contract.

7. RISK ASSESSMENT

A risk assessment must be conducted annually on all systems which process, store or transmit DMV information. Risk assessments must be documented at least every three (3) years or upon significant change to the system or environment. Risk assessment results must be provided to the CISO within 30 days of completion.

8. INCIDENT REPORTING

The Contractor shall immediately notify the DMV CISO/Designee of any actual or suspected security event involving DMV information accessed or obtained under this Contract. The Contractor shall cooperate fully with DMV to comply with the incident reporting requirements within Civil Code section 1798.29 and SAM section 5340.4.

The Contractor shall thoroughly investigate all unauthorized or suspected unauthorized access, use, and/or disclosure of information obtained under this Contract. DMV reserves the right to participate in the investigation of any information security incident involving its data and may conduct its own independent investigation, and the Contractor shall cooperate fully in such investigation.

The Contractor shall provide a preliminary report within three (3) working days of discovery of breach or unauthorized use or disclosure. The report shall include, but not be limited to, the information specified above, as well as any pertinent preliminary information. The Contractor shall then provide a full written report of the investigation to the DMV CISO and Privacy Officer within ten (10) working days

of the discovery of the breach or unauthorized use or disclosure. The report shall include, but not be limited to, the information specified above, as well as a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure.

DMV reserves the right to take corrective action at any time.

9. BREACH OR DISCLOSURE OF DMV INFORMATION

Disclosure of any DMV information to any person or entity not specifically authorized in this Contract is strictly prohibited. Personnel assigned to work with DMV's confidential information shall not reveal, share, or divulge to any person or entity any of the confidential information provided under this Contract, except as authorized or required by law.

DMV shall not be held liable for any breach of Contractor systems that results in the release of any information provided by DMV. Contractor agrees to indemnify and hold harmless DMV, its officers, and representatives from and against any liability, losses, costs, damages, or expenses (including but not limited to attorney fees) resulting from any claims arising from the performance of this Contract, including but not limited to any and all liability, damages, costs, expenses, or attorney fees resulting from a breach of security of the system as defined in the California IPA unless such damages are determined to be the result of the negligence of DMV, its officers, employees, or representatives.

In the event of a breach caused by the Contractor, the Contractor shall be responsible for sending out any and all notifications to individuals whose personal information is breached as defined in the Civil Code section 1798.29 and SAM section 5340.4. Contractor shall bear all costs and expenses associated with sending out any such notices, and will strictly comply with the requirements of Civil Code section 1798.29. In the event Contractor fails to send out the requisite notices, DMV in its sole discretion may notify all affected individuals, and Contractor shall bear all costs and expenses arising from any notifications sent out by DMV.

The DMV CISO shall review the content of any and all notifications and written approval must be obtained before notification can be made under this Contract.

C. PHYSICAL SAFEGUARDS

1. ACCESS CONTROL

The Contractor shall ensure information in all forms, such as, but not limited to CDs, DVDs, USB flash drives, or other removable media must be stored in areas physically secure and free from access by unauthorized persons as described in this Contract.

The Contractor shall ensure computer monitors, printers, hard copy printouts, or any other forms of information accessed or obtained under the performance of this Contract must not be viewed by the public or other unauthorized persons as described in the Contract.

2. SUPERVISION OF DATA

DMV information in paper form shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office. Unattended means that information is not being observed by an employee authorized to access the information. DMV information in paper form shall not be left unattended at any time in vehicles or planes and shall not be checked in baggage on commercial airplanes.

3. ESCORTING VISITORS

Visitors to areas where DMV information is contained shall be escorted and DMV information shall be kept out of sight while visitors are in the area.

4. REMOVAL OF DATA

DMV information must not be removed from the premises of the Contractor except with express written permission.

D. TECHNICAL SAFEGUARDS

1. DATA RETENTION AND DESTRUCTION

DMV information must be retained for the minimum necessary to perform the required business function.

All data received by the Contractor under this Contract and any data created, copied, attributed to data received shall be destroyed when no longer needed for the business function for which they were obtained, or within 10 calendar days of termination of this Contract. Data must be destroyed in accordance with the requirements specified NIST Special Publication (SP) 800-88, Guidelines for Media Sanitization.

2. ENCRYPTION

Confidential, sensitive, or personal information shall be encrypted in accordance with Federal Information Processing Standards 140-3, Security Requirements for Cryptographic Modules.

3. DATA AT REST AND IN TRANSIT

All DMV information at rest and in transit must be encrypted in accordance with the security and privacy provisions specified within this Contract.

4. ENDPOINT PROTECTION

All workstations, laptops and other systems that process, store, or transmit DMV information must install and actively use endpoint protection with automatic updates scheduled at least daily.

5. VULNERABILITY MANAGEMENT

Systems which store, process, or transmit DMV information must be scanned for vulnerabilities monthly, and when new vulnerabilities potentially affecting the system are identified and reported. Vulnerabilities by severity must be remediated within the following timeframe:

- Critical (3 business days or less)

- High (21 days)
- Medium (60 days)
- Low (90 days)

The CISO must be notified within 24 hours if critical vulnerabilities cannot be remediated within the required timeframe.

6. INTRUSION DETECTION

All systems which store, process, or transmit DMV information that are accessible via the Internet must be protected by a comprehensive intrusion detection and prevention solution.

7. WARNING BANNERS

All systems which store, process, or transmit DMV information must display a warning banner stating that data is confidential, systems are logged, and system use is for business purposes only by authorized users. User must be directed to log off the system if they do not agree with these requirements.

8. IDENTIFICATION

All users accessing DMV information must be issued unique user identification.

9. PASSWORD CONTROLS

Passwords must be a minimum 15 characters and must be composed of a minimum one character each from the following four groups:

a. Upper case letters (A-Z)

b. Lower case letters (a-z)

c. Arabic numerals (0-9)

d. Non-alphanumeric characters (punctuation symbols)

Passwords must be changed at least every 180 days.

10. USER ACCOUNTS

User accounts must be immediately disabled or deleted upon personnel termination or a change in assigned duties which no longer require access to DMV information.

11. MULTI FACTOR AUTHENTICATION

Multi factor authentication must be enabled for all users.

12. SESSION LOCK

Systems must not be left unattended and logged on. Systems must be configured to prevent access by initiating a session lock after no more than 10 minutes of inactivity. Session locks must be retained until the user reestablishes access using established identification and authentication procedures.

13. CHANGE CONTROL

The Contractor shall notify the DMV 30 days prior of any changes to systems, hardware, software, applications, file structure, data, or record layout which process, store, or transmit DMV information. The DMV shall notify the Contractor of any changes to DMV systems, hardware, software, applications, file structure, data, or record layout which process, store, or transmit information in the performance of this Contract at the discretion of the DMV.

14. AUDITING

The Contractor shall maintain an audit trail and record data access of authorized users and the authorization level of access granted to information based on job function. Said logs must be made available to the DMV upon request. The Contractor shall allow audits or inspections by individuals authorized by the DMV at the Contractor premises during regular business hours, with seven (7) business days prior notice for purposes of determining compliance with the terms of this Contract.