California Department of Motor Vehicles
Memorandum of Understanding
County Data Center (CDC)

This Memorandum of Understanding, hereinafter referred to as MOU, is between the Department of Motor Vehicles, State of California, hereinafter referred to as DMV, and the El Dorado County Information Technologies, 360 Fair Lane, Placerville, CA 95667, hereinafter referred to as IT. The IT will provide local government agencies, hereinafter referred to as Requester, on-line access service to DMV. The following terms and conditions will be followed by the identified parties of this MOU:

1. This MOU is subject to any restrictions, limitations, or conditions enacted by the California State Legislature which may affect the provisions or terms herein in any manner.
2. No alteration of the terms herein shall be valid unless made in writing and signed by the parties hereto. No oral understanding or agreement, not incorporated herein, shall be binding on any party.
3. At the DMV's sole discretion, the DMV may immediately and unilaterally suspend or cancel this MOU if the IT has failed or refused to comply with any terms for the security of data. The suspension or cancellation shall remain in effect until the DMV determines that there is satisfactory compliance.
4. The term of this MOU is effective from the date of final approval by the DMV Information Services Branch Chief or Designee and is subject to immediate cancellation and termination of access if **data is negligently or intentionally misused**. Termination without cause may be made by either party upon thirty (30) days prior written notice of such termination. Notice is effective five (5) days from the date sent by facsimile (FAX) transmission or five (5) days from the date of mailing. Termination initiated by the IT must be directed to the attention of DMV's Information Services Branch Electronic Access Administration Unit Manager.

   The address and telephone number are:

   Department of Motor Vehicles
   Manager, Electronic Access Administration Unit

P.O. Box 942890, Mail Station H-225
Sacramento, CA 94290-0890
(916) 657-5582
(916) 657-5907 (FAX)

5. The IT agrees to pay for any loss, liability or expense, including attorney fees, expert witness fees and court costs, which arises out of or relates to the IT acts or omissions regarding its obligations hereunder, where a final determination of liability on the part of the IT is established by a court of law or where settlement has been agreed to by the IT. This provision may not be construed to limit the IT rights, claims, or defenses which arise as a matter of law or under any other provision of this Agreement. This provision may not be construed to limit the sovereign immunity of the IT.
6. IT and its officers, agents and employees shall act in an independent capacity and not as officers, agents or employees of DMV.
7. DMV will provide the IT database information by means of direct network access. Services provided by DMV include, but are not limited to, technical, administrative, informational and network management access services.
8. IT shall not provide on-line service to a Requester without prior notification that the Requester has an assigned requester code and an approved DMV MOU. If DMV denies, terminates, or cancels approval of an Requester, DMV shall contact IT to terminate the Requester's service, and IT shall not thereafter extend service to that Requester unless and until all deficiencies identified by DMV have been resolved and written approval from DMV has been secured by IT.
9. IT agrees to establish security procedures to protect DMV records and access to confidential or restricted information as identified in California Vehicle Code Section §1808.47:

> "Any person who has access to confidential or restricted information from the department shall establish procedures to protect the confidentiality of those records. If any confidential or restricted information is released to any agent of a person authorized to obtain information, the person shall require the agent to take all steps necessary to ensure confidentiality and prevent the release of any information to a third party. No agent shall obtain or use any confidential or restricted records for any purpose other than the reason the information was requested."

IT shall ensure that each IT employee having direct or incidental access to DMV records has signed an Information Security Statement, Form INF 1128. The security statement shall be maintained on file for the life of the account and for two years following the deactivation or termination of the account. This completed form and list must be made available to DMV upon request.

10. Pursuant to California Civil Code (CCC) §1798.29, IT will utilize secured communication circuits whenever DMV records containing personal information is transmitted. If the Internet is used for intrastate communication that include DMV records, all electronic communications must, at minimum, utilize Secure Socket Layer (SSL) and 128-bit encryption protocols, or more secure methods.
11. IT shall within one (1) business day notify the Policy and Information Privacy Section Manager regarding any indication of known, suspected and/or questionable misuse or unauthorized access or disclosure of confidential or restricted DMV information at:

    Department of Motor Vehicles
    Manager, Policy and Information Privacy Section
    P.O. Box 942890, Mail Station H-225
    Sacramento, CA 94290-0890
    (916) 657-5583
    (916) 657-5907 (FAX)

12. In the event of any breach of the security of the IT system or database containing the personal information of California residents, the IT shall bear all responsibility for providing notice of the breach to the affected residents as required by CCC §1798.29. The IT shall bear all costs associated with providing this notice, and shall also be responsible for providing identity theft prevention services to the affected California residents. These protections include, but are not limited to, providing credit monitoring services for each affected resident for a minimum of one year following the breach of the security of the system maintained by the IT. In addition, the IT agrees to comply with all federal and California state law, including all of the provisions of the California statutes and Title 13 of the California Code of Regulations.
13. IT shall not sell, assign, or transfer any DMV information except as specified within this MOU.
14. IT shall maintain a current list of authorized Requesters that utilizes the IT for access to DMV files. This list shall be made available to DMV upon request.
15. IT agrees to accommodate DMV's request for an inspection, review or audit immediately upon request from DMV or DMV's representative and to allow on-site audits during

regular business hours for purposes of determining compliance with the terms of this MOU.

16. As part of any audit performed by the DMV of the IT, the DMV acknowledges that it will have access to certain IT information. " IT information" means any data or information, in any form, including but not limited to information reflecting and/or relating to system or network planning, design, development, processes, or procedures. The DMV shall ensure that:

    a. All IT information, and any audit report based thereon, is strictly confidential;
    b. DMV will access, use, and/or retain IT information for purposes of the DMV audit only; and
    c. DMV will not disclose IT information, or any audit report thereon, to anyone, except authorized recipients or as required by law.

17. IT will implement and maintain the security of its system and components used for retrieval, transmittal, storage and services used in conjunction with DMV records, as described in the documentation provided to and approved by DMV.

18. DMV reserves the right to change conditions and/or security requirements to keep pace with the development and enhancements of security, telecommunications and database technology. The IT reserves the right to submit a proposal to DMV to change conditions and/or security requirements to keep pace with the developments and enhancements of security, telecommunications and database technology.

19. IT shall ensure that all terminals, systems, storage media and network components used for **DMV information** access or services meet and maintain DMV's security requirements, **and are approved by DMV prior to implementation. All changes to systems, storage media and network components used for DMV information access or services must be reported to and approved by DMV in writing prior to implementation.**

20. The cost and maintenance of all communication lines shall not be the responsibility of DMV.

21. The DMV network security architecture requires the ability to identify each Requester by means of terminal, individual User Identifier, system, and/or transaction identifiers. The IT computer system must control access by each Requester to specific terminals, users, systems, and/or transactions, as appropriate to the protocol and interface employed, which shall be identified using an agreed upon naming convention according to the National

Institute of Standards Technology (for example, TCPIP, VPN, etc.). Requesters' access must be restricted to unique specified identifiers in the DMV communication interface.

22. IT shall ensure that any access control program administered either by the IT or Requester, consists of, at a minimum, a unique individual user identifier and user selected passwords for each person be utilized on every system capable of DMV access. At a minimum, verification of manually keyed unique User Identifier and passwords shall be required for initiation of access.

23. Record access information shall be electronically logged and securely stored (i.e. password protect, administrative rights, encrypted) for a period of two years from the date of the transaction. The information shall be preserved for audit purposes for a period of two years, and will include, at a minimum, the following:

    a. Transaction and information codes (i.e., ANI, DAK, R60)
    b. Requester codes
    c. Record identifiers (i.e., DL Number, License Plate Number or Vin)
    d. All individual user identifiers, including individual user ID who can access and view DMV record information
    e. Dates and times of the transactions
    f. Terminal ID and locations
    g. Cross reference to the corresponding supporting documentation, (i.e., file/case number, account number, inventory/control number)
    h. Name of the subject of the request
    i. Purpose of the request (inquiry and/or update)
    j. Date the record was received from DMV

I have read and understand the Memorandum of Understanding and agree to abide by the terms and conditions herein.

Executed at: ______________________, ______________, ____________________
City County State

Approved By: ______________________________________ Date: ________________
Authorized Signatory (Manager/CEA/Deputy Director)

Print Name: ____

Title: ____

STATE OF CALIFORNIA
Department of Motor Vehicles

Approved By: ______________________________________ Date: ________________
Debi Orr, Section Manager
Electronic Access and Security Section