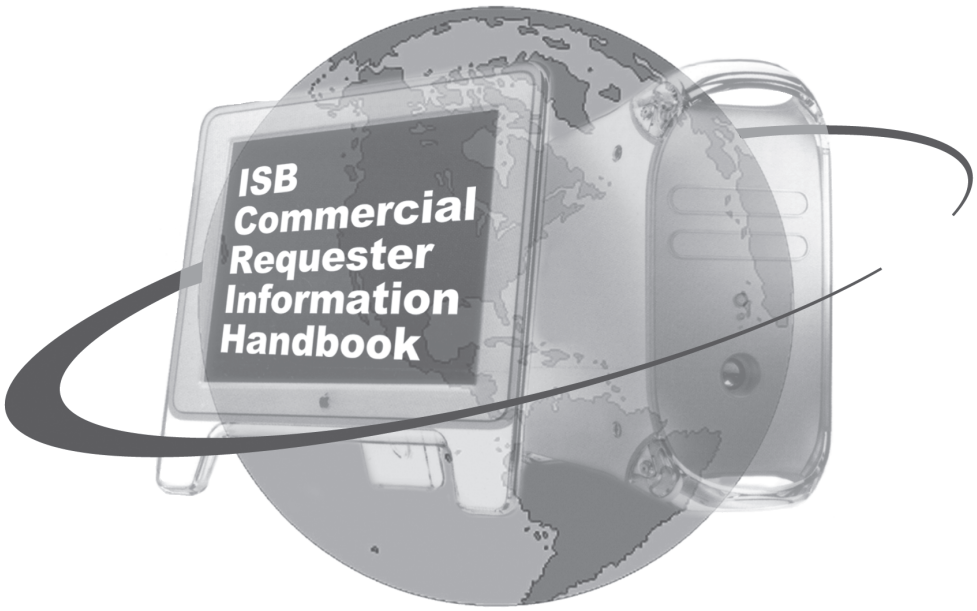
State of California

DEPARTMENT OF MOTOR VEHICLES

# COMMERCIAL REQUESTER INFORMATION HANDBOOK




Communication Programs Division

INFORMATION SERVICES BRANCH


## Foreword

The Department of Motor Vehicles takes great pride in its ability to fulfill its mission. We remain dedicated to making service to all customers the cornerstone of our operations.

Fulfilling our mission is a complex task, and extends beyond customer service. We must protect the privacy of individuals whose information is contained in our massive database, while at the same time meet the legitimate business needs of our customers. The electronic transmission of the information must be secure. The balance between privacy protection and access to public records is guided by state and federal laws and regulations, and it is on this foundation that the Information Services Program operates.

In this Commercial Requester Information Handbook, our goal is to answer questions about what is needed to become a Commercial Requester Account (CRA) Holder. It is our intent to facilitate the application process and make you aware of your responsibilities as a CRA holder. We have rules and requirements that must be met, and every account is subject to an audit. Included in this publication is a copy of the Terms and Conditions (INF 1230) that all CRA holders must agree to. Any failure to adhere to these terms and conditions or to the security requirements, also contained within this book, may result in the department taking adverse action against your account.

We try to make the process of obtaining records smooth and timely. That is our goal, and commitment to you as a customer of the department. At the same time, we ask that you take your responsibilities to heart, and for every record you request from us, treat the information carefully and safeguard it. Use it only for the purpose for which you are approved to request it. Follow the rules and procedures outlined in this handbook and in regulations. Ensure your employees are also following the requirements, it's YOUR account at stake.

Please read this booklet. The information contained in here is fundamental to understanding the requirements for a CRA and obligations once it is approved. And, let us know what you think about it. There is a survey card in the back. Your comments will help us improve future editions.

Information Services Branch
Department of Motor Vehicles

# TABLE OF CONTENTS

# TABLE OF CONTENTS

# THE INFORMATION SERVICES PROGRAM

## INFORMATION SERVICES BRANCH

### MISSION STATEMENT

In support of Department and Division goals, it is the mission of the Information Services Branch to provide information and support to internal and external customers and:

- Protect privacy by ensuring record security.
- Ensure service is provided in a courteous, secure, expeditious, and understandable manner.
- Utilize technological improvements to provide information in an efficient, cost effective manner.
- Operate with a bias for action, continuously improving information products, services, and sales consistent with the Department's mission and customer needs.
- Provide first class service and build a positive image in dealing with Information Services clients.
- Maximize the talents and efforts of skilled staff and actively encourage their professional development.

January 2002

The Department of Motor Vehicles (DMV) is authorized by California Vehicle Code (CVC) Section 1810.2 to establish Commercial Requester Accounts (CRA) and issue requester codes for the purpose of requesting information from the department's files.

The department has two (2) types of requesters:

(1) Requesters who are pre-approved to receive information from the department to fulfill a legitimate business need pursuant to one of the following statutes: CVC 1808 et seq., CVC 4465, CVC 22851.8, California Civil Code Sections 3067-3075, inclusive, and Harbors/Navigation Code Sections 500-509, inclusive.

(2) Requesters who are not pre-approved and request departmental record information on a one-time or occasional basis as authorized under CVC 1808 et seq.

Commercial Requester Accounts are established for applicants who:

- Have a legitimate business need for obtaining DMV information
- Properly complete and return the appropriate forms
- Pay the required application fee
- Provide an acceptable bond, if required
- Establish and maintain logs which track the receipt, use and dissemination of DMV information
- Maintain the confidentiality of the information provided

A requester may be approved for driver license, vehicle or vessel registration, financial responsibility and/or occupational licensing information. A requester code also limits access based on a requester's statutory authority to receive any of the following:

- Residence address
- Mailing address (when available)
- Basic record information (without address)
- Residence address with post notification to the subject

As a requester you may request information directly from the department. Information from the department can be requested via hardcopy, magnetic tape, on-line, or indirectly through an approved information provider or reseller (see page 6.002 for additional information on resellers).

## THE INFORMATION SERVICES PROGRAM *(continued)*

A requester code may be denied if the proposed use of the information is not related to the legitimate business needs or commercial purposes of the requester. The requester code may be cancelled immediately if the requested information is used for a purpose other than the purpose for which the requester code was issued. All requesters are required to maintain the security of the information received from the department and to protect it from unauthorized access. Additionally, as a Commercial Requester you may be subject to an audit by the department.

**Information submitted to the department on an application to obtain a Commercial Requester Account is public record. However, some information contained in these records is classified as confidential, trade secret, or personal pursuant to state or federal statute and is exempt from disclosure.**

# RECORD RELEASE

**Public record information** may be released by DMV to any person for an authorized purpose. An authorized business purpose may include, but is not limited to, vehicles/vessel lien sales, underwriting auto insurance policies, and pre-employment screenings. A driver license/identification (DL/ID) record contains information obtained from an individual's DL/ID application, abstracts of convictions, accidents, and any actions taken by the department. A vehicle/vessel registration (VR) record contains information relating to the registration of a vehicle or vessel. CVC §1808 describes the above as open to public inspection.

**Residence addresses** are confidential and information will only be released as authorized by CVC §1808.21, which states that any residence address in any record of the department is confidential, and shall not be disclosed to any person, except a court, law enforcement agency, other government agency, or as authorized by statute. Other confidential information include physical and mental conditions, controlled substance offenses (VC 1808.5), and Social Security Numbers (VC 1653.5(f). (Please visit our website at www.dmv.ca.gov for more information.)

**Statutes authorizing residence address release include, but are not limited to the following:**

1. Financial Institutions licensed by the state or federal government to do business in the State of California which state under penalty of perjury that they have obtained a written waiver of California Vehicle Code (CVC) §1808.21 signed by the individual whose address is requested. [CVC §1808.22 (a)]
2. Insurance Companies licensed to do business in California when the company, under penalty of perjury, requests the information for the purpose of obtaining the address of another motorist or vehicle owner involved in an accident with their insured or requests the information on an individual who has signed a written waiver of CVC §1808.21. [CVC §1808.22 (b)]
3. Attorneys who state under penalty of perjury, that the motor vehicle registered owner's or driver's residential address information is necessary in order to represent his or her client in a criminal or civil action which directly involves the use of the motor vehicle. [CVC §1808.22 (c)]
4. Vehicle Dealers licensed to do business in the State of California if the dealer, or its agent, under penalty of perjury, requests and uses the information only for the purpose of completing registration transactions and documents. [CVC §1808.23 (b)]
5. Any person who, under penalty of perjury requests and uses the information as permitted under subdivision (h) of California Civil Code (CCC) §1798.24, if the request specifies that no person will be contacted by mail or otherwise at the address included with the information released. [CVC §1808.23 (c)]
6. Vehicle Manufacturers licensed to do business in the State of California if the manufacturer, or its agent, under penalty of perjury, requests and uses the information only for the purpose of safety, warranty, including a warranty issued in compliance with CCC §1795.92, emission, or product recall if the manufacturer offers to make and makes any changes at no cost to the vehicle owner. [CVC §1808.23 (a)]
7. Any person who certifies that the residence address information will only be used to notify the registered and legal owners and all persons known to claim an interest in the vehicle of an impending lien sale or intent to dispose of the vehicle. Each residence address requested from the files of the DMV will be required by and will be used pursuant to the applicable statutes including but not limited to the following: CVC §22658, 22851, 22851.8, 22852, CCC §3068 through 3072 and Harbors and Navigation Code §500-509.

# PERMISSIBLE USE(S)/PURPOSE

Federal legislation, the Driver's Privacy Protection Act (Title 18, United States Code, Section 2721-2725), makes confidential any information contained in a motor vehicle record unless the information is requested and used for a "permissible use". A "permissible use" includes:

1. **Government/Law Enforcement Agent** – For use by any private person or entity acting on behalf of a Federal, State or local agency in carrying out the functions of the government/law enforcement entity.
2. **Motor Vehicle or Drivers Safety and Theft** - For use in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; performing monitoring of motor vehicles; motor vehicle parts and dealers; motor vehicle market research activities, including survey research; removal of non-owner records from the original owner records of motor vehicle manufacturers.
3. **Legitimate Business For Purposes of Preventing Fraud** – For use in the normal course of business by a legitimate business or its agents, employees, or contractors but only to verify the accuracy of personal information submitted by an individual to the business, its agents, employees or contractors; and if information as so submitted is not correct or is no longer correct, to obtain the correct information but only for the purposes of preventing fraud by pursuing legal remedies against, or recovering on a debt or security interest against an individual.
4. **Civil, Criminal, Administrative or Arbitral Processing** - For use in connection with any civil, criminal, administrative, or arbitral proceeding in any Federal, State, or local court or agency, or before any self-regulatory body including service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a Federal, State or local court.
5. **Research and Statistical Reports** - For use in research activities, in producing statistical reports so long as the personal information is not published, re-disclosed or used to contact individuals.
6. **Insurance Purposes** - For use by an insurer or insurance support organization, or by a self-insured entity, its agents, employees or contractors, or in connection with claims investigation activities, antifraud activities, rating or underwriting.
7. **Towed or Impounded Vehicles** – For use in providing notice to owners of towed or impounded vehicles.
8. **Private Investigator/Security Service** - For use by any licensed private investigative agency or licensed security service for any purpose permitted under this section.
9. **Any Other Use Specifically Authorized Under California Law** – For any other use specifically authorized under the law of the State that holds the record if such use is related to the operation of a motor vehicle or public safety as long as an authorizing statute can be cited.

STATE OF CALIFORNIA
DMV
DEPARTMENT OF MOTOR VEHICLES
*A Public Service Agency*

## *Information Services Branch*
## COMMERCIAL REQUESTER ACCOUNT TERMS AND CONDITIONS

Department of Motor Vehicles (DMV) reserves the right to modify the following terms and conditions at will.

### A. GENERAL

By applying for a Commercial Requester Account to access DMV information, you, the "Requester" agree to the following:

1. The term of the Commercial Requester Account shall be for two years from date of approval and may be renewed biennially or extended by the department.
2. Requester shall not sell or transfer ownership of a vehicle or vessel if the information received from the files of the DMV indicates a Department of Justice stop ("DOJ STOP"). Requester shall notify the local police regarding the vehicle or vessel whenever the location of the vehicle or vessel is known.
3. Requester agrees to defend, indemnify and hold harmless the DMV and its officers, agents and employees from any and all claims, actions, damages or losses which may be brought or alleged against the DMV, its officers, agents or employees by reason of the negligent, improper, or unauthorized use or dissemination by the Requester or its officers, agents, or employees, of information furnished to the Requester by the DMV or by reason of inaccurate information furnished to the Requester by the DMV unless the Requester can show that the DMV was originally furnished accurate information from the reporting source.
4. Requester shall not represent itself as an agent or employee of the DMV. Requester shall not use any DMV trade mark or service mark, indicia or any substantial similarity thereto or acronym in a manner likely to cause confusion that Requester's services are associated with or are that of the DMV.
5. Requester and its designees shall use DMV information for purpose(s) for which it requests an account and is approved by the DMV. Any other use(s) is strictly prohibited and will subject the Requester and its designees to termination of account as well as civil and criminal penalties.
6. Requester shall notify DMV in writing within ten (10) days of any changes including but not limited to address, telephone number, contact person, closure or sale of business.
7. Commercial Requester Account and attendant Requester code(s) are personal to the Requester and no rights or responsibilities under this agreement are assignable by Requester.
8. Resale of DMV information is prohibited. Requester shall not store, combine or link department information with any database for resale or for any business purpose(s) not specified on the application for a Commercial Requester Account approved by the DMV. Continued storage of information is permissible to comply with federal or state record retention requirements.
9. Requester's access to DMV information may be modified and/or terminated
   - immediately with cause
   - without cause upon 30 days notice by either party

## B. SECURITY

1. Requester shall comply with all DMV security requirements relating to its Commercial Requester Account. Requester understands that the DMV reserves the right to amend or enhance its requirements and continuance of a Commercial Requester Account is contingent upon Requester's compliance with the updated criteria. Security requirements are available at www.dmv.ca.gov (click on "Other Services"). It is the responsibility of the account holder to periodically review this website, but no less than once every 6 months, for any future updates or enhancements to the security requirements. Requester affirms that it has, or has access to, the internet that will allow them to view the website for current and updated security requirements.
2. Requester shall be responsible for safeguarding the information received and shall restrict access to this information to its employees, agents or parties with whom it contracts. Requester agrees to be held responsible for any misuse of the information by its employees, agents or parties to whom the information was entrusted.

## C. RESIDENCE ADDRESS

If receiving residence address information, the Requester shall secure a surety bond in the amount of $50,000 and is subject to the provisions of California Code of Regulations (CCR) §350.24.

## D. FEES

1. Requesters receiving information directly from the DMV shall be charged a fee pursuant to CCR §350.44 and shall be billed monthly for information received.
2. The amount listed on the invoice is due and payable upon receipt. Failure to remit the appropriate payment could result in termination of your requester privileges and may include a referral to a collection agency.

## E. DISPUTES

1. Requester may withhold payment of any disputed charges. A "charge" is not disputed until Requester provides the DMV a written explanation of the disputed charge within 30 days of invoice date. If the DMV determines the charges are valid, the Requester will be notified and shall pay all such charges within (10) ten days.
2. Requester consents to jurisdiction of California courts and the Requester agrees to Sacramento County, California as the forum selected for judicial review of its rights relating to its account under these terms and conditions. Any disputes regarding the Requester's account shall be adjudicated pursuant to the laws of the State of California.
3. The person authorized to complete and sign the application on behalf of the Requester may be held personally responsible to the DMV for any debts and obligations arising under this agreement.

## F. INSPECTION OF RECORDS

1. Requester shall keep its records required pursuant to CCR §350.18(b) (4) and CCR §350.48 at the business address provided to the DMV.
2. Requester's place of business shall be available for an electronic or manual audit (of records required to be retained) immediately upon request from the DMV or the DMV's representative.
3. Requester understands that failure to respond timely to an audit report with findings, may result in inactivation/ cancellation of the Requester code.

# CHAPTER ONE

# COMMERCIAL REQUESTER ACCOUNTS

| | |
|---|---|
| **1. Who can apply for a Commercial Requester Account (CRA)?** | Any person or business who has a legitimate business need for obtaining DMV information can apply for a requester code account. (See page 6.001 for definition of legitimate business need). For further information please see California Code of Regulations (CCR) 350.02(1). |
| **2. How do I apply for a CRA and requester code?** | You must submit a completed application for a commercial requester code account. |
| **3. Which form(s) do I need to complete for a CRA application?** | See "Forms", page 6.003, for a list of forms that are required. |
| **4. Are there different types of accounts and what do I need for each type?** | Yes. Currently, you can apply to be an End-User or Reseller/Service Provider (Contact the Account Processing Unit at (916) 657-5564 for additional information). |
| **5. Is there a fee for the Commercial Requester Account?** | Yes. Fees to apply for a requester code account are due with the application and renewable every 2 years, the fees are:<br><br>Basic Record (Without residence address) - $50<br><br>With residence address - $250 (a surety bond of $50,000 is also required). (See page 1.003) |
| **6. How will I know if my application is approved?** | You will receive an approval letter in the mail once your application is approved. The letter will contain your requester code number(s). Approval letters will not be faxed or sent electronically. |
| **7. When will my account expire?** | A Commercial Requester Account is valid for twenty-four (24) months from the date of approval. |
| **8. Will I be notified to renew my account?** | The Account Processing Unit will notify account holders approximately ninety (90) days prior to the expiration of the account by forwarding a renewal package to the contact person identified on the account. **To avoid any delay in service, please ensure that any change to your contact person is reported (See item 12.)** |

# COMMERCIAL REQUESTER ACCOUNTS *(continued)*

| | |
|---|---|
| **9. Are the fees refundable if I don't qualify for a requester code account?** | The $50.00 application fee is a nonrefundable fee. If you applied for a CRA account with residence address, and you do not qualify, we will refund the $200 portion of the fee. |
| **10. How much do the records cost?** | • Each electronic record - $2 for vehicle registration, $2 for driver license<br>• Driver license and vehicle registration records - $5 each<br>• Copies of microfilmed records or photos:<br>  • DL - $20 for each copy<br>  • VR - $20 for each year.<br>• Requests for large volumes or bulk requests - $100 per thousand copies, in addition to computer run time and programming. |
| **11. When am I required to report changes to my account?** | You are required to report any changes, such as, a change in corporate name, corporate officers, sole proprietor, Doing Business As (DBA), telephone number, account contact, street or mailing address, billing contact, or any change in any other information on the original account application. |
| **12. How do I report changes to my account?** | Changes to your account must be reported on form INF 1106. You must notify DMV of any changes to your Commercial Requester Account within ten (10) working days of the change(s). Please contact the unit listed below to request copies of the form or visit our website at *www.dmv.ca.gov*, then go to "Other Services" and click on Commercial Requester Account. |
| **13. Who do I contact if I have questions about my application, or to check on the status of my application?** | You can contact the Account Processing Unit (APU) at (916) 657-5564. Please allow at least two weeks for processing. |
| **NOTE:** | **Once your account is approved and requester code(s) is/are assigned, please include this number(s) on all correspondence to the department concerning the specific account.** |

## COMMERCIAL REQUESTER ACCOUNTS *(continued)*

## SURETY BOND INFORMATION

| | |
|---|---|
| **14. Do I need a bond to apply for a Commercial Requester Account?** | You will need a surety bond **only** if you are issued a requester code and authorized to receive residence address information. |
| **15. What is the amount of the bond?** | The surety bond must be in the amount of $50,000. The bond must be continuous and made payable to the Department of Motor Vehicles. |
| **16. Where can I obtain a surety bond?** | The "Commercial Requester Account Surety Bond", INF 1132 will be mailed to you upon approval for address information. You should only submit the form when requested by the department after you have been approved for residence address. This is the only form that will be accepted. Many insurance companies can issue a surety bond. **DMV will only accept bonds issued by insurance companies licensed to do business in California.** |
| **17. What information should the bond contain?** | The "Commercial Requester Account Surety Bond" form INF 1132 must be completed in its entirety. It must contain the date and signature of an authorized employee of the surety company. The bond must read exactly how the commercial requester account reads.<br>Examples are:<br>• Sole owner should have the individual's name as well as the DBA (doing business as) on the account.<br>• Partnerships should have all partners' individual names and the DBA on the account.<br>• Corporations should have the name of the corporation only (if the corporation name and DBA are identical) or the corporation name and DBA if different on the account.<br>• Limited Liability Corporations should read the Limited Liability Corporation (LLC) and DBA on the account.<br>**Note: The bond will be returned to the principal if any information is incorrect or not completed properly.** |
| **18. How long must the bond be maintained?** | The bond must remain valid and in effect during the account period in order to continue to receive residence address information. If the bond expires during that time, your account will be downgraded to receive record information without address until you reestablish the bond and it is in full force. |

# CHAPTER TWO

# CUSTOMER INFORMATION SECURITY REQUIREMENTS

## PART I

## General Provisions

By signing the Commercial Requester Account Application (INF 1106) and/or Commercial Requester Account Service Provider Application (INF 1106V), Requester agrees to comply with these Security Requirements and any additional requirements deemed necessary by the Department of Motor Vehicles (DMV).

DMV reserves the right to amend or enhance its requirements and continuance of a Commercial Requester Account is contingent upon Requester's compliance with the updated criteria.

A PowerPoint presentation *"Confidentiality of DMV Information"* is available upon request. If additional information is required or you would like a copy of the presentation, please contact the DMV's Electronic Access Administration Unit at (916) 657-5582.

California Vehicle Code (CVC), Division 1, Article 3, Sections 1800-1825, *"Records of the Department"* is available at **WWW.LEGINFO.CA.GOV/CALAW.HTML.**

*CVC §1808.45. The willful, unauthorized disclosure of information from any department record to any person, or the use of any false representation to obtain information from a department record or any use of information obtained from any department record for a purpose person or organization for purposes not disclosed in the request is a misdemeanor, punishable by a fine not exceeding five thousand dollars ($5,000) or by imprisonment in the county jail not exceeding one year, or both fine and imprisonment.*

*CVC §1808.46. No person or agent shall directly or indirectly obtain information from the department files using false representations or distribute restricted or confidential information to any person or use the information for a reason not authorized or specified in a requester code application. Any person who violates this section, in addition to any other penalty provided in this code, is liable to the department for civil penalties up to one hundred thousand dollars ($100,000) and shall have its requester code privileges suspended for a period of up to five (5) years, or revoked. The regulatory agencies having jurisdiction over any licensed person receiving information pursuant to this chapter shall implement procedures to review the procedures of any license which receives information to ensure compliance with the limitations on the use of information as part of the agency's regular oversight of the licensees. The agency shall report noncompliance to the department.*

*CVC §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.*

# CUSTOMER INFORMATION SECURITY REQUIREMENTS

California Code of Regulations (CCR), Title 13, Division 1, Chapter 1, Article 5, *"Requesting Information From the Department"* is available at: **WWW.CALREGS.COM.**

California Civil Code (CC), Section 1798.80-1798.84, **inclusive.**

United States Code (USC), Title 18, Part I, Chapter 123, *Driver's Privacy Protection Act of 1994,* Section 2724. (a) Cause of Action. – A person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains, who may bring a civil action in a United States district court. (b) Remedies – The court may award – (1) actual damages, but not less than liquidated damages in the amount of $2,500; (2) punitive damages upon proof of willful or reckless disregard of the law; (3) reasonable attorney's fees and other litigation costs reasonably incurred; and (4) such other preliminary and equitable relief as the court determines to be appropriate.

## PART II

## Security Requirements

1. A "Requester" is any person issued a requester code. **Part II is applicable to all Requesters.**

2. Requester shall maintain the security and integrity of any information it receives and shall maintain records and documents to justify and support proper use of requested information. All Requesters are required to establish and maintain daily logs and source document that track the receipt, use and dissemination of DMV information.

3. Requester shall notify DMV's Information Services Branch, Policy and Information Privacy Section, by telephone, at (916) 657-5583 within one (1) business day if fraud or abuse is suspected or confirmed, or the security of the requester code is compromised.

4. A written notification containing all facts shall be prepared by the Requester within three (3) business days and mailed to the Policy and Information Privacy Section. (See Part IV)

5. Requester shall require every employee and/or the system administrator, having direct or incidental access to DMV records, to sign a copy of the *Information Security Statement,* (INF 1128), upon initial authorization for access and annually thereafter.

6. Requester shall maintain signed *Information Security Statement,* (INF 1128), forms at the Requester's worksite for at least two (2) years following the deactiviation or termination of the authorization and shall be available to the DMV upon demand.

7. Requester shall restrict the use and knowledge of requester codes and operational manuals to persons who have signed an *Information Security Statement,* (INF 1128).

## CUSTOMER INFORMATION SECURITY REQUIREMENTS *(Continued)*

8. Requester shall maintain and make available to DMV upon demand, a current list of names of persons authorized to access DMV records, terminal identifiers (i.e., termid/netname), and the number of users for each terminal, if applicable.

9. Requester shall ensure that video terminals, printers, hard copy printouts, or any other form of duplication of DMV information that is located in public access areas shall be placed so that the public or other unauthorized persons cannot view the information.

10. Access terminals displaying DMV data shall display a "sign-on banner" containing some variation of the following admonishment: "WARNING: Unauthorized access or misuse of data may result in adverse action and/or criminal prosecution".

11. Requester shall ensure that DMV information is not electronically transmitted to anyone unless the file is protected from disclosure during transport. Encryption for this purpose shall use algorithms in compliance with published National Institute of Standards and Technology (NIST), American National Standards Institute (ANSI) and Internet Engineering Task Force (IETF).

12. Requester shall ensure that all information received from DMV files is destroyed once its legitimate use has ended. The method of destruction shall be in a manner that it cannot be reproduced or identified in any physical or electronic form.

13. Requester shall not disclose its DMV assigned requester code, orally, in writing or electronically, to anyone that is not in the direct employment of Requester or has not signed the *Information Security Statement*, (INF 1128) other than a DMV approved Service Provider.

14. Requesters are required to implement and maintain adequate physical security for DMV information received (in any format), equipment, and systems that access DMV information.

15. Requester shall prevent unauthorized access administratively and/or electronically, including developing policies, procedures, and training of users on all information security including compliance with California Civil Code §1798.82.

16. Requester shall ensure that systems and DMV data transmitted or stored off-site, regardless of format, must be physically protected from unauthorized access or use during transit and in storage. Physical access to network components, servers and data storage devices must be restricted to authorized and identified staff.

## PART III

## Additional Security Requirements for:

## A. Confidential Residence Address Access

1. Any Requester who is authorized to access and use confidential residence address information shall protect the confidentiality of any residence address received from DMV records pursuant to CVC §1808.47 and shall comply with additional security requirements contained in this section.

## CUSTOMER INFORMATION SECURITY REQUIREMENTS *(Continued)*

2. Prior to being approved to access and use confidential residence address information, a Requester shall provide the state or federal statute that authorizes or requires DMV to release confidential residence address information and the use of any confidential information obtained shall be limited as provided in the identified statute.

3. Requester shall not use confidential residence address information obtained for any direct marketing purpose.

4. Requester shall maintain a log of each request for two (2) years from the date of the request. The log shall be immediately available to DMV upon demand. The log format shall provide the following in the order presented:

   a. Requester code used to make the request.
   b. Date of request.
   c. Type of information requested.
   d. Points of identification used for the request (e.g., license # and DOB).
   e. Business reason for the request.

5. Requester shall not obtain or use any confidential or restricted information for any purpose other than the purpose approved by the DMV.

### B. Service Providers

1. A "Service Provider" is any Requester who is performing a service to another pre-approved Requester as identified in 2 or 3 below:

2. Service Providers who are performing a contracted service (Agent) on behalf of another pre-approved Requester shall maintain a log of each request for information for a period of two (2) years from the date of the request. The log shall be immediately available to DMV upon demand. The log format shall provide the following in the order presented:

   a. Date of request.
   b. Type of information requested.
   c. Whether residence address information was provided.
   d. Identity of whom the information was provided.

3. Service Providers who are providing a Pass Through/Reformat Service (Vendor/Reseller) for DMV pre-approved Requesters shall maintain a log of the request for a period of five (5) years from the date of the request. The log shall be immediately available to DMV upon demand. The log format shall provide the following in the order presented:

   a. Date of request.
   b. Type of information requested.
   c. Whether residence address information was provided (including "intermediate vendors").
   d. Proposed use of information as approved by DMV.

4. Service Provider shall provide DMV information only to other pre-approved Requesters and shall include its assigned requester code as part of each inquiry submitted, in a format specified by DMV, in additional to the assigned requester code of the pre-approved requester.

## CUSTOMER INFORMATION SECURITY REQUIREMENTS *(Continued)*

5. Service Provider (Agent) may retain information only as required to fulfill its contractual agreement with the pre-approved requester as indicated on Agent Authorization Form(s), INF 03 or Parking/ Toll Road Violation Agency Notification on file with the Department.

6. Service Provider shall make available to the DMV upon demand a copy of the contract between the Service Provider and the pre-approved requester.

7. Service Provider (Agent) shall notify DMV of any changes, additions and/or deletions regarding your Agent Authorization.

8. Service Providers (Agents) who are authorized to update DMV information shall comply with the following Update Security Requirements, which may include, but are not limited to:
   a. Non-repudiation program application for the electronic update to DMV's database(s).
   b. ***On-Line Security Administration*** and electronic validation programs.
   c. Restrict transaction types as necessary to ensure the user is authorized for updates.
   d. Encryption, a Virtual Private Network, and use of Special Carriers transporting hardcopy or cartridge/reel computer tapes.
   e. Use is restricted to an assigned device identifier that is electronically verified and validated against DMV's security table. Special Permit Holder acting as an Agent for approved government Requesters who are processing update transactions to DMV's driver license and vehicle/vessel registration database(s) is restricted to an assigned device identifier that is electronically verified and validated against DMV's security table.

### C. On-Line (Direct) Access – Direct Requester

1. A "Special Permit" is a signed agreement between DMV and a Requester authorizing on-line (direct) access to the DMV's electronic database. In addition to any other applicable section, a Special Permit Holder shall comply with all additional on-line security requirements contained herein.

2. Special Permit Holder shall maintain the security and integrity of DMV information and the on-line information service system.

3. Special Permit Holder's computer system shall be capable of identifying all terminals and controlling access to Special Permit Holder's computer system at all times.

4. Each terminal accessing Special Permit Holder's computer system shall be a termination point in the communications network as approved by the DMV.

5. No terminal or system shall act as an intermediate communications node for other remote systems.

## CUSTOMER INFORMATION SECURITY REQUIREMENTS *(Continued)*

6. Special Permit Holder shall submit, for DMV approval, the current Special Permit Holder's and all terminals (if applicable) Network Topology containing functional system descriptions, and a security narrative that describes how each security requirement is to be met by the Special Permit Holder. If employing more than one type of system, documentation shall be supplied for each type. A Network Topology and the security narrative shall be supplied:
   a. Upon Special Permit Holder's initial on-line information service request.
   b. A minimum of thirty (30) days, in advance, for DMV's review of any changes being made in hardware or software systems that affect Special Permit Holder/End User communication access to DMV's database(s).
   c. Upon request by DMV.

   Special Permit Holder may be required to submit accreditation documentation for DMV's approval of an original/renewal application. DMV will consider the information required by this paragraph to be proprietary and confidential.
7. Special Permit Holder shall automatically terminate a session logon once it commences and nothing is entered into the computer system or no data record is received in any continuous ten (10) minute time period. Upon automatic termination, any data on the screen will be removed and not restored without initiation of a new session logon. This termination shall be obvious to the user.
8. Special Permit Holder shall maintain an electronic file of the User ID, requester code, date and time of every occurrence where Special Permit Holder has automatically terminated an access due to non-use within a ten minute time period. These records shall be kept for two (2) years from the date of the access termination and shall be available to DMV upon request.
9. Special Permit Holder shall secure, control, and monitor all devices and software that contain or produce unique identification codes used by Special Permit Holder or DMV for verification of authorized access.
10. Special Permit Holder shall secure, control, and monitor all systems, equipment, circuits, business related communication software and application software on storage media, etc., that may allow unlawful and/or unauthorized access to DMV information.
11. Special Permit Holder shall terminate access to Requester and shall notify DMV's Electronic Access Administration Unit (see Part IV) within one (1) working day when Requester refuses compliance with, or violates any security requirement.
12. Special Permit Holder shall electronically log each transaction transmitted to Requester. Information electronically logged shall include:
    a. Transaction code.
    b. Information code.
    c. Requester's requester code.

## CUSTOMER INFORMATION SECURITY REQUIREMENTS *(Continued)*

d. Record identifiers (e.g., driver license number, vehicle license number, vehicle identification number).
e. Individual User ID.
f. The date and time of the transaction.
g. Date record received from DMV.
h. Requester's terminal location.
i. Residence address information code (to be established to indicate whether or not address was received).

This log requirement is in addition to Part III, ***B.2.*** and ***B.3***. but may be combined if retention is consistent. Log records shall be kept for two (2) years from the date of the transaction. Special Permit Holder shall be capable of selectively listing inquiry transactions based on specific criteria, defined by DMV, including, but not limited to, Requester's requester code and User ID. A printed report or electronic file shall be submitted to DMV upon request. Special Permit Holder is solely responsible for the accuracy of information so stored and for meeting all audit trail requirements.

13. Access to any logged data, required under this addendum, shall be restricted to Special Permit Holder's Security Administrator and DMV approved audit personnel. Access to the logged data by any other user or application must be prevented by an active access control system performing the functuality defined in ***Part II Section D***. Any deviations must have advanced written approval by DMV.

14. Special Permit Holder shall not change approved system configuration, and shall not allow End Users to make changes or modifications which would alter the approved system configuration, without prior written approval from DMV.

15. Special Permit Holder shall not have a compiler or an assembler connected to the production computer accessing DMV information.

16. Special Permit Holder shall maintain a current list of Special Permit Holder employees' authorized direct or incidental record access. The list shall be available to DMV upon request.

17. DMV's production records shall not be accessed for testing. DMV maintains test database(s) that can be utilized by Special Permit Holder. Additional test records will be created for Special Permit Holder upon written request. Requests to use the test database(s) must be approved in advance by contacting the DMV's Electronic Access Administration Unit (see ***Part IV***).

18. Special Permit Holder shall install and maintain cost for establishing on-line access between DMV and the Special Permit Holder and costs for any other equipment or software needed for installation and maintenance, shall be the sole responsibility of the Special Permit Holder. Upon thirty (30) days notice, the Special Permit Holder agrees that DMV may move the Special Permit Holder's connection located at DMV as required. Costs for any DMV required movement will be borne by DMV.

## CUSTOMER INFORMATION SECURITY REQUIREMENTS *(Continued)*

19. If service to the Special Permit Holder is terminated, any modem or other equipment furnished by the Special Permit Holder to DMV shall be returned to the Special Permit Holder at the Special Permit Holder's expense.

20. The Special Permit Holder shall obtain DMV information on-line according to the type of connection approved by DMV. Data flow between the Special Permit Holder and Requester must comply with DMV's established technical and security requirements to prevent unauthorized access to DMV information. Approved connectivity will be documented and will specify the type of connectivity approved and the security requirements associated with that connectivity.

21. The Special Permit Holder shall use electronic time-of-day and day-of-week blocks to restrict system access by the Requester to the Requester's days and hours of inquiry as approved by DMV.

22. The Special Permit Holder shall include its assigned requester code as part of each inquiry submitted, in a format specified by DMV and shall use the appropriate requester code(s) as required by the DMV transaction being processed.

23. On-line information service may be affected by ongoing maintenance requirements that result in unannounced shutdowns of the communication network and database files. These may be planned or unplanned depending upon the problem and type of maintenance required.

24. A Special Permit Holder provides on-line access or access and update to DMV files for an authorized Requester. Special Permit Holder may act as a Service Provider to themselves and function as a Requester for the purposes of this section, with prior written approval of DMV, provided that:
    a. An organizational chart is submitted that identifies a clear separation of the Service Provider and the Requester functions.
    b. Service Provider and the Requester utilize separate requester codes on all transactions.
    c. All Service Provider and Requester requirements specified apply to the respective functions.
    d. Security administration configurations and system design for combined Service Provider/Requester systems are approved by DMV.
    e. Establish independent system hardware for the Service Provider and Requester functions.
    f. Company owners, partners, or corporate principal officers shall not serve as Access Control or Review Administrator.
    g. Access Control Administrator duties and Review Administrator duties are performed by a different individual.

25. The Special Permit Holder may be required to have Access Control and Review Administrators individually bonded.

# CUSTOMER INFORMATION SECURITY REQUIREMENTS *(Continued)*

## D. On-Line Security Administration

### 1. Security Adminstration

Security administration is the responsibility of the Special Permit Holder or Internet Host. This function includes both Access Control Administrator and Review Security Administrator. The Special Permit Holder or Internet Host shall ensure that all requirements of security administration are met.The Special Permit Holder or Internet Host will provide the name and title of the individual responsible for the Access Control Administrator and Review Security Administrator's functions on the Commercial Requester Account Service Provider Application.

### 2. Security Administrator

The Security Administrator functions may not be delegated to the Requester without prior written approval from DMV. If these functions are delegated to Requester, the following required steps must be completed.

a. A Special Permit Holder shall submit a written request for approval to DMV's Electronic Access Administration Unit (see ***Part IV***) prior to delegating Access Control Administration to a pre-approved requester. The written request shall include:
   i. A statement that the Requester will be responsible for the Access Control Administration functions instead of the named Reseller.
   ii. A description of the applicable business purpose for the request.
   iii. The name and title of the individual designated as the Access Control Administrator.
   iv. The name and title of the individual designated as the Review Security Administrator.
   v. Signature of Requester authorized to sign for the Commercial Requester Account.
   vi. An approval line for the signature of the Reseller and the signature of the Information Services Branch Chief for concurrence and approval.
   vii. A Network Topology, security narrative that complies with all of the security, technical, and programming requirements.
   viii. An On-line Special Permit Personal History Questionnaire completed by the Requester who signed the written request, the Access Control and Review Security Administrators.

### 3. Access Control Administrator

a. Verification of a unique individual identity and access authority shall be performed prior to forwarding any inquiry transaction to DMV. The Access Control Administrator shall administer this function, hereinafter referred to as "session logon". Individuals working with DMV information shall be subjected to the following basic three-step process known as "access control":

   Step 1. ***Identification:*** Each individual must have a unique User ID authorized by the Access Control Administrator.

## CUSTOMER INFORMATION SECURITY REQUIREMENTS *(Continued)*

Step 2. ***Authentication:*** Each individual must be asked to provide a type of confidential or personal information, such as a password, voice recognition, retinal scan, etc., that will verify the identification of the person seeking access to DMV's files.

Step 3. ***Authorization:*** The first two steps in the access control process are tests for the user to prove their identity. Authorization shall be controlled by software that limits the functions a particular user can perform.

b. If an individual is not authorized for the type of transaction requested, the Access Control Administrator shall terminate the transaction and notify the Requester and the Review Administrator. If the Access Control Administrator receives a transaction from an unauthorized individual, the Access Control Administrator shall terminate the transaction and attempt to identify the unauthorized individual.

c. The Access Control Administrator shall require a user authentication method. This method shall be no less secure than a manually entered User ID and password validated by the security administration system. The security administration system shall electronically enforce the user authentication method utilized. (See ***Section D.3***. – **User ID/Password Standards**).

d. Passwords used to perform authentication service, shall be stored on the security administration system in an encoded format. The encoded format shall be achieved using a Data Encryption Standard (DES) algorithm. The encryption shall be one way only (i.e., the encryption cannot be removed from the password.)

e. An electronic file containing User ID, date, and time for each occurrence of a password change shall be maintained.

f. Assignment by the Access Control Administrator of an electronically enforced unique default user authentication to each individual upon initial access. The default user authentication shall be utilized in cases where an authorized individual has forgotten their password or where an authorized individual has incorrectly attempted a session logon three (3) times and has had their access revoked. Access Control Administrator shall ensure that the default user authentication shall not be capable of being utilized for subsequent access by an individual.

g. Any alternative process for individual access control requires prior written approval from DMV and must be at least as secure as the user authentication method required in this section.

h. Access to the user authentication data by any other user or application must be prevented by an active access control system performing the functionality defined in this section. Any deviations must be approved, in advance, by DMV.

i. The Access Control Administrator shall revoke a User ID, and notify the Review Administrator, within 24 hours of becoming aware of any of the following circumstances.

   i. The holder of the User ID no longer requires access to DMV information.

## CUSTOMER INFORMATION SECURITY REQUIREMENTS *(Continued)*

ii. The holder of the User ID authorized for DMV record information access leaves the employ of Special Permit Holder or Requester.
iii. The holder of the User ID is guilty of unauthorized disclosure or misuse of DMV information.
iv. The holder of the User ID does not comply with DMV's information security requirements.
v. Requester access is terminated. Access Control Administrator shall revoke the User ID of all Requester employees utilizing the On-line Information Service.

j. The Access Control Administrator shall be responsible for appropriate training of general security issues regarding User ID and password management of each individual accessing information under this addendum.

k. Individual's User ID will be assigned and controlled by Access Control Administrator. Access Control Administrator shall require each individual to utilize the user authentication method to initiate each session logon as defined in ***Section D.1***. Before an inquiry transaction may be initiated, the individual's User ID must be validated and accepted by the security administration computer system.

l. The Access Control Administrator shall maintain an electronic file of all individuals accessing DMV information. Each electronic file shall include:

i. The date access was initially granted.

ii. Business name, address, and phone number.

iii. Requester code.

iv. Individual's name and User ID.

v. The date and reason access was revoked (if appropriate).

This information shall be updated as changes occur and shall be provided to DMV upon request. A two (2) year history of any and all changes to the information shall be kept for all Individuals with current on-line information access. For inactive users, this information shall be retained for two (2) years from the date on-line information access was terminated.

**4. Review Security Administration**

a. A Review Security Administrator, hereinafter referred to as the "Review Administrator", reporting to a different manager within the organization than the Access Control Administrator, shall administer the review responsibilities identified in this section.

b. All logon attempts, whether successful or unsuccessful, shall be electronically logged and monitored by the Review Administrator on a daily basis. An unsuccessful logon attempt is any attempt to log on to the computer system that is rejected because of an incorrect User ID and/or user authentication method. The Requester's access shall be revoked after three (3) consecutive unsuccessful logon attempts.

## CUSTOMER INFORMATION SECURITY REQUIREMENTS *(Continued)*

c. The Review Administrator shall notify DMV in writing within three (3) working days of any individual who submits three (3) consecutive unauthorized transactions. Mail the notification to the DMV's Policy and Information Privacy Section (see ***Part IV***).

d. The Review Administrator shall notify the Special Permit Holder within one (1) working day of any of the occurrences noted by the Access Control Administrator defined in ***Section D.1***. The Review Administrator shall set up a report using criteria to ensure the above requirements are being met. These criteria shall include, but are not limited to, date, time, location of attempted access, and reason revoked. This report shall be submitted to DMV upon request, in the media agreed upon.

e. The Review Administrator shall monitor the on-line information access activities of all individual users having DMV record access. Sufficient information shall be electronically logged so that the following checks and actions can be performed. The Review Administrator shall date and initial (or electronically key) an acknowledgement of logged records indicating the following checks have been performed on a monthly basis.

   i. Complete log information has been kept for each unauthorized inquiry transaction attempt.
   ii. Complete access control information has been kept for each completed transaction.
   iii. Complete log information has been kept for each transaction attempt for every occurrence of an invalid requester code being entered. An invalid requester code is defined as any requester code that is:

      1) **not** authorized by DMV,
      2) **not** valid for the user initiating the transaction,
      3) **not** valid for a particular transaction, or
      4) **not** valid for a particular Requester device identifier (wrong terminal/ communication line.)

f. The Review Administrator shall check for patterns that might indicate unauthorized attempts to gain access to DMV files. Review Administrator shall investigate suspected unauthorized access attempts. Should unauthorized access attempts be confirmed. Review Administrator shall immediately alert DMV by telephone at (916) 657-5583, with a written follow-up to DMV Electronic Access Administration Unit within one (1) working day (See ***Part IV***).

g. The Review Administrator shall keep a record of all active terminals, the addresses of all terminal locations, the names of all authorized persons for each terminal location, and the names of any deleted or inactivated users for each location. A report of the above information shall be provided to DMV upon request, in the media agreed upon.

# CUSTOMER INFORMATION SECURITY REQUIREMENTS *(Continued)*

**5. User ID/Password Standards**

a. Password authentication requires a unique identification component (User ID) assigned by Requester and a confidential password component. Both components are required for authentication.

b. Assigned of User ID's and default passwords must be accomplished using a secure process, for example, do not e-mail in clear text.

c. DMV User ID requirements:

i. User ID must be unique to each individual and not assigned to groups or job locations.
ii. User ID's shall be revoked after three (3) consecutive unsuccessful logon attempts. Re-authorizing the User ID requires verification of the user's identity.
iii. "Default" passwords, known only to the user, may be used for the purpose of re-setting the account. Default passwords may not be used to conduct business.

d. Password requirements:

i. Passwords must be validated by the system against the User ID for each logon to the system.
ii. The owner of the User ID shall choose passwords.
iii. The user must manually enter passwords. Programming function keys or use of other automated means to enter passwords shall be prohibited. Application programs shall not allow the password to be saved.
iv. Passwords must contain six (6) or more characters.
v. Passwords must consist of both alpha and numeric characters.
vi. Passwords shall not utilize symbols or punctuation marks (#, %, !, etc.).
vii. Passwords must expire in 60 days or less.
viii. Passwords shall not be displayed in a readable manner on the screen when keyed.
ix. After a password has been changed, the system must prevent the user from changing it again within two (2) days. (An administrator may re-authorize the user, if necessary, during this time.)
x. The system shall prevent the user from re-using the password within twelve (12) password history iterations.
xi. Passwords stored in the program must be encrypted using DES, or equal/better, one-way-only encryption.
xii. Passwords must never be written down or displayed in plain text. This requirement can be enforced by written policy.

# CUSTOMER INFORMATION SECURITY REQUIREMENTS *(Continued)*

## E. On-Line (Direct) Access – Indirect Requester

1. Any Requester who obtains on-line (direct) access to DMV information from a ***Special Permit Holder*** shall, in addition to any other applicable sections, comply with all security requirements contained in this section.

2. Logon access to the Special Permit Holder's computer from all the Requester terminals shall require a unique user authentication method controlled by the Special Permit Holder. This method shall be no less secure than a manually entered password validated against user's ID for each authorized user (person) at the Requester's site. Passwords shall be unique to the individual and shall be held in confidence. Passwords shall be a minimum of six (6) characters in length, shall be made up of a combination of alphabetic and numeric characters, but cannot be all alphabetic or all numeric, and shall be chosen so that they cannot be readily identified with the person using them (i.e., their name/initials, family members, etc.).

3. Passwords shall be changed at least every 60 days. Passwords shall be changed immediately if it is suspected another individual has knowledge of an individual's password. The same person shall not use a password more than once within a twelve-iteration period. Passwords shall not be written down or otherwise kept in a location where they can be seen or easily obtained by anyone other than the person to whom they belong.

4. The Requester shall manually key the unique assigned individual user ID and the unique individual password to initiate each access session. Each user ID shall only be assigned to one person for their exclusive use and shall not be shared.

5. The Requester shall notify the Special Permit Holder immediately upon terminating authorization for an individual's access to DMV records. The Requester shall maintain a list of individuals whose authorization has been terminated, containing the reason for and the date of access termination. Names contained in the list shall not be purged for at least two (2) years from the date the individual's status becomes inactive.

6. The Requester's communications network shall be the termination point of any record information received from DMV. No terminal or system shall act as an intermediate communications node for other remote systems outside of the Requester's organization.

7. Data flow between the Requester and the Special Permit Holder must include the appropriate security measures and technical requirements to prevent unauthorized access to DMV information.

8. The Requester shall control access to their system and prevent unauthorized user access to the Special Permit Holder's system.

## CUSTOMER INFORMATION SECURITY REQUIREMENTS *(Continued)*

9. The Requester shall submit a written request to DMV for review and approval for special inquiry transactions that release specific data elements for statistical purposes or require a specific criteria to effect a yes or no business response, or release only the record status information. A special addendum may be required to specify the purpose and use of the information, applicable statutory authority, restrictions on use of the data, security requirements, and payment of fees if due, for programming or for records to be paid by the Requester.D.

### F. Internet

When use of Internet-based technologies is included in **any** portion of the information-processing environment, all Requesters shall comply with all requirements specified in ***California DMV Security Requirements for the Internet*** handbook.

### G. Batch Processing by:

1. When use of Virtual Private Network (VPN) or File Transfer Protocol (FTP) based technologies is included in any portion of the information-processing environment, all Requesters shall comply with any requirements specified in ***VPN Services Offerings Manual*** and the *VPN Client Manual*. The VPN Services Offerings Manual is available by clicking on the link above or you can contact the DMV Electronic Access Administration Unit at (916) 657-5582 to have a copy of either manual sent to you.

2. All data transferred to/from DMV must terminate behind an internal firewall and the system must be protected and on a trusted network. DMZ configurations **do not** meet this requirement.

3. VPN batch customers must change their Resource Access Control Facility (RACF) password at least every 35 days.

4. Addition RACF password standards include:

    a. Passwords must be at least 5 characters long.
    b. Passwords can be any combination of alphabetic, numeric or special characters.
    c. Passwords cannot be reused for 32 iterations.
    d. Passwords will be locked out of the system after 5 erroneous password attempts.
    e. Passwords can be changed any time.

5. Minimum hardware/software requirements are identified in the ***VPN Services Offerings Manual.***

6. Security requirements require 3DES encryption for Router-to-Router customers.

7. Firewall and network configuration changes may affect your VPN connections. DMV's technical staff will assist when possible.

8. As technology improves/changes, additional security concerns and changes may be required.

## CUSTOMER INFORMATION SECURITY REQUIREMENTS *(Continued)*

9. Requesters will be required to submit a completed ***VPN Questionnaire*** and ***VPN Customer Information Listing*** prior to conversion of batch program(s) output.
10. Output data set names are emptied and reallocated recurrently. Therefore, requesters must retrieve their output files prior to sending their input files.
11. There is a maximum limit of 50,000 records that a customer can send for each process, per day. Anything larger must be coordinated in advance.
12. Input files are processed Monday through Friday, excluding DMV non-business days (holidays, weekends, etc.). The ***DMV holiday schedule*** is available by clicking on the link or contacting the Electronic Access Administration Unit at (916) 657-5582.
13. The daily production schedule begins at 4:30 p.m. (Pacific Time). Input files sent by this time will be available the next business day, by 7:00 a.m. (Pacific Time).
14. All VPN connections must at a minimum meet the following requirements in order to protect the integrity and confidentiality of DMV data. These requirements apply to ALL VPN connections, including router-to-router, lan-to-lan, and client connections.
    a. At least one firewall system must be located between any server that hosts applications, provides access to or stores DMV information and each external network entry point.
    b. Firewalls must include, at a minimum, provisions for packet filtering, application gateway security mechanisms, and circuit-level gateways.
    c. If a server is accessed through the same Internet access point used to access the Internet from internal workstations, the firewall implementation must also include proxy services and/or address translation.
    d. When a server is used to store, transmit, or process DMV information, the firewall systems employed must be located so that all communications with the Internet must pass through two differently-authored firewall systems separated by an isolated network.

### PART IV

**For further information or assistance with:**

| | |
|---|---|
| Processing Forms | Account Processing Unit – H221<br>PO Box 944231<br>Sacramento, CA 94244-2310<br>(916) 657-5564 |
| Electronic Access Methods | Electronic Access Administration Unit – H225<br>PO Box 942890<br>Sacramento, CA 94290-0890<br>(916) 657-5582 |
| Policy/Information Privacy | Policy and Information Privacy Section – H225<br>PO Box 942890<br>Sacramento, CA 94290-0890<br>(916) 657-5583 |

## CUSTOMER INFORMATION SECURITY REQUIREMENTS *(Continued)*

| | |
|---|---|
| **1. What are the available methods to receive information from DMV?** | Information can be received either directly from DMV (i.e., hardcopy, magnetic tape, on-line) or indirectly from a department-approved reseller/service provider. For a current list of approved resellers/service providers, contact the Account Processing Unit at (916) 657-5564. |
| **2. Can I use the information received from DMV for any purpose?** | Information obtained from DMV can only be used for the legitimate business purpose approved by the department. The department's approval letter will contain the business purpose for which you were approved. (See page 6.001 for a definition of legitimate business need.) |
| **3. Can I retain, combine, link or store the information I receive from DMV?** | Information received from DMV cannot be retained, stored, combined, and/or linked with any other data on any database for any subsequent reproduction, distribution, or resale. The individual record may be stored and maintained either manually or electronically for the purpose for which it was requested and for as long as your legitimate business use requires. (See IMPORTANT NOTE below). |
| **4. If I am a "consumer reporting agency" as defined in 15 USCS 1681a (f) of the Fair Credit Reporting Act (FCRA) and must retain information to comply with FCRA requirements, how long can I keep this information?** | As a "consumer reporting agency", records obtained from DMV can be stored exclusively to respond to inquiries for information contained in consumer reports and verification of that information if disputed. You may retain the information for a "reasonable" period of time to respond to customer inquiries. DMV interprets "reasonable" as 60 days from the date the information was received. If the information is undisputed, it must be destroyed after the 60-day retention period. If the information is disputed, the records must be destroyed upon the resolution of the dispute. |
| **5. What do I do with the record information when it is no longer needed?** | Commercial requesters are responsible for destroying DMV record information containing personal information, such as; name, driver license or identification number, or physical characteristics, etc., by shredding, erasing or modifying the personal information to make it unreadable or undecipherable as provided in Civil Code Sections 1798.80, 1798.81, and 1798.82. |
| **IMPORTANT NOTE** | **Residence addresses received from department records shall not be used for any direct marketing or solicitation for the purchase of any consumer product or service. [CVC§ 1808.23 (d)]** |

## CUSTOMER INFORMATION SECURITY REQUIREMENTS *(Continued)*

| | |
|---|---|
| **6. If I have someone acting as my agent, can I release confidential information to that person?** | If confidential or restricted information is released to any agent of a person authorized by the department, the person shall require the agent to take all steps necessary to ensure confidentiality of this information. No agent shall obtain or use any confidential or restricted records from requester code holders for any purpose other than the reason the information was requested. Reasons for requesting information are limited to those stated on the approved account application. |
| **7. Are there any DMV forms that must be signed by someone acting as my agent or by my employees?** | Yes, an "Information Security Statement", form INF 1128, **must** be maintained on file for each agent, performing work on behalf of the requester. The INF 1128, is also required for all employees authorized to access DMV information. These forms **must** be maintained at the worksite and be available to the DMV auditors upon request. |
| **8. Do I need to have any written procedures in place for information security?** | You are required to establish written procedures to protect the confidentiality of the information received from DMV. CVC §1808.47 states: Any person who has access to confidential or restricted information from DMV shall establish procedures to protect the confidentiality of those records. |
| **9. Where must these procedures be kept?** | The established security procedures must be maintained on site and available to the department's auditors. |
| **10. Do I need to have anyone in charge of securing this information?** | Yes. You should appoint someone to be in charge of maintaining the security of DMV information. Please be able to provide the name, title, and telephone number of that person upon request. |
| **11. Are there any other security requirements I or my employees must be aware of if accessing DMV information by computer?** | The following has been prepared to assist in complying with the security requirements:<br>• Remember, account holders are personally responsible for all activity occurring under their user identification while signed on to the DMV computer.<br>• Do not write passwords down or tell your password to anyone. Passwords are not to be shared among individuals or groups.<br>• Always log off the terminal each time the terminal is left unattended.<br>• Passwords should be changed at least every 60 days or less, to help prevent illegal access. |

## CUSTOMER INFORMATION SECURITY REQUIREMENTS *(Continued)*

| | |
|---|---|
| **11. Are there any other security requirements I or my employees must be aware of if accessing DMV information by computer?** *(continued)* | • DMV information **should only** be **requested and** used for the legitimate business need for which it was approved.<br>• Do not have your terminal screen visible to anyone that is not authorized to view the information.<br>• DMV information **must** be properly destroyed when it is no longer needed for the reason for which it was originally requested.<br>• Any terminals accessing DMV information **must not** be in areas open to the public. Video screens containing DMV information must be facing away from the public.<br>• Printed records, microfilmed records, and any records stored to any electronic media (diskette, hard drive etc.), must be protected from unauthorized access and viewing.<br>• Requester code(s) and any personal identification numbers used by employees **must** be protected from unauthorized use. |
| **12. Do I need to keep any logs of the information I request?** | Yes. You must establish and maintain daily logs and source documents which track the receipt, use, and dissemination of DMV information. *These logs and documents **must** be available to DMV auditors upon request.* |
| **13. What information must the log contain?** | The log must contain the following information for every transaction:<br>• Requester code<br>• Date of request<br>• Name of the subject of request<br>• Information requested (Driver License, Vin/Hin #, Vehicle/Vessel Plate #)<br>• Reason or purpose for the request and supporting documentation as necessary<br>• Cross-reference to the corresponding supporting documentation, e.g., file/case #, account #, inventory/control #, etc. |
| **14. How long must the log be retained?** | The log and required documentation must be kept for two years from the date of the request by any requester who requests or receives confidential information not for resale in accordance with California Code of Regulations 350.48(c). |

## CUSTOMER INFORMATION SECURITY REQUIREMENTS *(Continued)*

| | |
|---|---|
| **15. Who should I notify if I suspect fraud or misuse of DMV record information?** | If fraud or misuse is suspected or confirmed, you must notify DMV's Information Services Branch, Policy and Information Privacy Section at: (916) 657-5583, within one (1) business day of discovery. A written notification containing all facts must be prepared by the requester within three (3) business days and mailed to:<br><br>Department of Motor Vehicles<br>Policy and Information Privacy Section, MS H225<br>P.O. Box 942890<br>Sacramento, CA 94290-0890 |

# CHAPTER THREE

# AUDIT REQUIREMENTS

The Compliance Audits Unit audits commercial requesters to ensure compliance with the requirements of CVC, California Code of Regulations (CCR) Title 13 and the terms and conditions of the Commercial Requester Account.

| | |
|---|---|
| **1. Will my account be audited?** | All Commercial Requester Accounts are subject to DMV audits. Any account may be audited regardless of the method used to request or receive the information (on-line, hardcopy, magnetic tape, etc.) or the type of information that the requester is authorized to receive (basic, residence address, mailing address or residence address with post notification).<br><br>Certain conditions may warrant an unannounced audit, however, in most cases DMV will contact the requester by telephone approximately 1 to 2 weeks in advance to schedule the audit. |
| **2. How are account holders selected?** | Audit requests that are referred to us because of complaints or investigations are considered a priority. The remaining audits are scheduled based on a selection criteria determined by the management of the Compliance Audits Unit. |
| **3. What happens during the audit process?** | The audit consists of:<br>• An entrance conference to explain the audit process<br>• Testing and review of supporting documentation<br>• An exit conference to inform you of any findings<br>• A written audit report<br><br>Typical audits take 4 to 6 hours for the conferences and on-site testing, however, some may require additional time. |
| **4. What do I need for the audit?** | The auditors will review your:<br>• Supporting documentation to show evidence of proper use<br>• Required logs (refer to page 2.007)<br>• Information Security Statements<br>• Listing of employees authorized to request information<br>• Listing of terminated employee authorization |

# AUDIT REQUIREMENTS *(continued)*

| | |
|---|---|
| **What do I need for the audit?** *(continued)* | • Billings or invoices from your re-seller/service provider<br><br>The supporting documentation must be kept at the physical place of business listed on the application or the branch location form (INF 1106BL) and shall be made available for audit. |
| **5. What is supporting documentation?** | Supporting documentation shows evidence of proper use of DMV information and it varies according to the type of business. We typically see the following:<br><br>**Insurance companies** provide policy numbers, accident reports, SR-1 information or insurance quotes.<br><br>**Law offices** supply us with a client information sheet, retainer agreement, accident report and court case number.<br><br>**Private investigators** provide us with case name, file numbers, client information and reports.<br><br>**Registration services** supply information related to the transaction processed such as fees collected, method of payment, date fees collected, cost to client.<br><br>**Dealers** pull their dealer jacket, purchase/lease agreement/odometer disclosure statement, release of liability, title, registration or a bill of sale.<br><br>**Towing** companies provide towing and lien sale data.<br><br>**Auto auctions** provide us with stock/inventory numbers, report of sale, and buyer/seller information. |
| **6. What happens after the audit?** | Once the audit is completed and reviewed by management, an audit report is issued. You may be required to respond in writing to the findings in the audit report and explain what corrective action has been taken to address the findings. Failure to respond to the audit report within the specified timeframe may result in the inactivation of your requester account.<br><br>Audits with findings (non-compliance with CVC, CCR, and the Terms and Conditions of the Commercial Requester Account or other applicable statutes) are subject to final determination by ISB management for adverse or corrective action (re-audit, monitoring, referral to legal office or referral to investigation). |

## AUDIT REQUIREMENTS *(continued)*

| | |
|---|---|
| **7. Can DMV take any other actions?** | If an audit discloses a violation of any provisions of the California Code of Regulations (CCR) Title 13, whether by omission or commission, DMV may have grounds to take action that may result in suspension or termination of access privileges of the requester. DMV may also pursue appropriate administrative, civil, and/or criminal action for any violations in accordance with CVC 1808.45 and 1808.46 and Title 13 of the CCR. |
| **8. Is there any thing else I should know about the audit?** | If the audit reveals violation(s) of CVC 1808.22 through 1808.47 and/or violation(s) listed under CCR Section 350.52 the requester may be subject to administrative or criminal action. |
| **9. If my account is terminated either voluntarily or involuntarily, what should I do?** | Whenever an account is terminated with or without cause, or voluntarily closed pursuant to CCR 350.16 (b), the department ***may*** require the holder to surrender all information and records retained pursuant to CCR 350.48 & 350.18 (b) (4) and (5) not later than the end of the third business day following the date of termination or closure. The notification to surrender the records must be included in the notice of revocation or termination. |
| **10. If my account is terminated and I am notified to surrender my records where should they be sent?** | Upon notification to surrender the records, they should be mailed to:<br><br>Department of Motor Vehicles<br>Compliance Audits Unit MS H230<br>P.O. Box 932345<br>Sacramento, CA 94232-3450 |

# CHAPTER FOUR

# MONTHLY BILLING STATEMENT

| | |
|---|---|
| **1. When will I be billed?** | Invoices will be mailed to appropriate account holders who receive information directly from the department no later than the 10th of the month. If you obtain information from a reseller, you will not receive an invoice from DMV. |
| **2. When is my bill due?** | The entire balance listed on the invoice is due and payable upon receipt. |
| **3. What do I submit with my payment to DMV?** | When remitting payment, you must return the bottom portion or stub of the ORIGINAL invoice. Do not send a photocopy of the stub, as this will cause delays in the remittance process. You must indicate your account number on the check or money order and make all checks or money orders payable to the DMV. Do not write below the automated scan line on the bottom of the stub as any marks in this area prevents your account from being updated expeditiously and can cause errors in posting to your payment. |
| **4. What happens if I do not pay my bill on time?** | Failure to remit the appropriate payment could result in the cancellation of your requester privileges and may include a referral to a collection agency or collection against your bond. Pursuant to California Code of Regulations 350.46 (a), your requester code will be revoked if any amount remains unpaid sixty (60) days after the invoice date. |
| **5. If I have a dispute about my bill, what should I do?** | If you dispute any portion of your bill you must notify us in writing within thirty-(30) days of the invoice date. |
| **6. Can I note any changes to my address on the payment stub?** | **No**. All changes to your account, including address changes should be submitted on **form INF 1106** to the address listed on the form. |
| **7. Who can I call if I have questions about my bill?** | You can call the Automated Billing Information Systems Unit at (916) 657-6474. |

# GENERAL QUESTIONS

| | |
|---|---|
| **Q) I am an attorney representing a client in a motor vehicle related incident (accident, lemon law, odometer roll-back, etc.). May I release the residence address to an attorney service or licensed Private Investigator to perform service of process?** | ***Attorneys for Motor-Vehicle Related Incidents***<br>A) Yes, the attorney service or licensed private investigator would become your agent. A signed INF 1128 (Information Security Statement) must be signed and retained at your worksite. |
| **Q) I am an attorney representing a client in a motor vehicle related incident. Can I pass DMV information on to my client?** | A) No. DMV record information can only be used by the attorney or their agent. |
| **Q) What is a branch location?** | ***Branch Locations***<br>A) An offshoot, lateral extension, or division with a separate physical location but under the same corporate number and ownership. |
| **Q) Are there separate application fees for branch locations?** | A) No. |
| **Q) I am an approved end-user to perform background or pre-employment screenings, without address, and my client is an approved account holder with address authority, can I use their requester code?** | ***Sharing Requester Code***<br>A) **No,** an account holder may not pass his requester code on to anyone except an employee or agent who has signed an Information Security Statement (INF 1128). |

## GENERAL QUESTIONS *(continued)*

| | |
|---|---|
| **Q) Is a background check or pre-employment screening considered re- selling DMV information?** | ***Background Checks/Pre-Employment Screening***<br>A) No. When DMV record information becomes a part of a compilation of other information (i.e., employment history, credit history, etc.), it is considered a business function by the end-user. ***If the only part of the background check is a DMV record this constitutes a resale and approval from the department must be obtained.*** |
| **Q) Are you required to have an account with DMV if you get record information from a department approved information reseller?** | ***Reseller/Service Provider***<br>A) Yes. A department approved information reseller is only authorized to release department record information to an approved requester account holder (i.e., end-user, and reseller). |

# GLOSSARY

| | |
|---|---|
| **[Account] Contact Person:** | ***DEFINITIONS***<br>The contact person must be an employee of the firm who is familiar with the account and have the authority and responsibility for problem resolution. This person must be available to DMV during normal business hours for questions or problems as they arise. |
| **Commercial Account Holder:** | An entity that has been approved by the department and issued a requester code to purchase information from DMV. |
| **Consumer Reporting Agency: (Fair Credit Reporting Act 15 U.S.C. §1681 et seq.)** | Any person which for monetary fees, dues, or on a cooperative non-profit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. |
| **End User:** | The Requester Account Holder for whose business use department information is obtained. An end user may be either the person requesting the information or another person on whose behalf the information is requested. |
| **Fair Credit Reporting Act 15 U.S.C. § 1681 *et seq.*** | Federal statute that was enacted to protect individuals from inaccurate or arbitrary information being documented in consumer reports. |
| **Legitimate Business Need:** | Legitimate Business Need. An authorized purpose for requesting, obtaining, disclosing or using information contained in a department record. |
| **Lien Sale:** | The sale of a vehicle when a person, who, under the laws of the state in which the sale will be conducted, has a claim on the property of another as security for the compensation to which the person is legally entitled for making repairs or performing labor upon; the furnishing of supplies or materials for; the storage or safekeeping of; and for the rental of parking space for; any vehicle. |
| **Mailing Address:** | An address, different from and reported separately from the residence address, where mail is to be delivered to the addressee. When the address used for mailing is the same as the residence address, it is considered to be a residence address. A mailing address is mandatory only when mail cannot be delivered to the reporting individual's residence address. |

# GLOSSARY *(continued)*

| | |
|---|---|
| **Public Record:** | California Vehicle Code Section 1808 and the Public Records Act (Government Code Section 6253 et al.), provides that information collected by the Department is generally considered public information and is subject to inspection by the public. Exceptions to this public disclosure obligation include: ***Personal Information*** and ***Confidential Information.*** |
| **Residence Address:** | The address reported to DMV by an individual as the place where that individual resides. This is confidential and only released pursuant to statute. |
| **Requester Code:** | A unique configuration of numbers or letters assigned by DMV to identify a requester(s). |
| **Reseller/Service Provider:** | A requester account holder who has been authorized by DMV to facilitate the legal transfer of information contained in a department record to any pre-approved requester. For information regarding Information Reseller/Service Providers, contact the Account Processing Unit at (916) 657-5564. |

# FORMS/CONTACT NUMBERS

The following forms are provided with the Commercial Requester Account Application package (INF 1133) or the Commercial Requester Account Service Provider Application package (INF 1133V). A hardcopy may also be provided by contacting the Account Processing Unit at (916) 657-5564:

| | |
|---|---|
| **INF 1106**<br>**Commercial Requester Account Application** | Complete this form if you will be using DMV record information for your own business use. (Example: Insurance Agent/Broker to underwrite insurance, background check/pre-employment company, Registration Service, Dealer/Manufacturer, etc.) This form must be completed to apply for an original requester account, renewal of an account, or to make changes to an existing account. |
| **INF 1106BL**<br>**Commercial Requester Account Branch Location** | Account holders with multiple branch locations needing different requester codes must complete this form. |
| **INF 1106V**<br>**Commercial Requester Account** | Complete this form if you will be accessing DMV record information to perform a legitimate business service on behalf of another CRA applicant (Example: pass thru/reformat (Reseller) or other contracted service (Agent). This form must be completed to apply for an original requester account, renewal of an account, or to make changes to an existing account. |
| **INF 1128**<br>**Information Security Statement** | This form must be signed annually by any individual who has access to information received from the department. It must be retained at the account holder's worksite for the length of time indicated on the form. ***Do not sent to DMV.*** |
| **INF 1132**<br>**Commercial Requester Account Surety Bond** | This form will be mailed to you once you have been approved for residence address access. |
| **INF 1184**<br>**Certification of Agency** | Any Vehicle Dealer Agent or Vehicle Manufacturer Agent who will be requesting residence address via Commercial Account to process registration transaction documents or recalls on behalf of a dealer or manufacturer, must have this form completed by all dealers/manufacturers the agent represents. |
| **INF 1230**<br>**Commercial Requester Account Terms and Conditions** | This form contains the terms and conditions an account holder must agree to in order to be approved for a commercial requester account. ***Do not sent to DMV.*** |

# FORMS/CONTACT NUMBERS *(continued)*

| | |
|---|---|
| **INF 03**<br>**Agent Authorization** | This form is to be completed and signed by each preapproved requester (government or commercial) for which a service provider will be providing a contracted service in which access to confidential residence address is requested. This form is not necessary if performing a pass-thru/reformat (reseller) service. |
| **Account Processing Unit**<br>**(916) 657-5564** | Requester Account Help, Questions or Changes |
| **Automated Billing Information Unit**<br>**(916) 657-6474** | Requester Account Billing Information |
| **Electronic Access/ Security Unit**<br>**(916) 657-5582** | File Transfer and On-line Access |
| **Policy/Information Privacy Section**<br>**(916) 657-5583** | Policies and Procedures regarding DMV record release and/or uses. Automation needs relating to the release of information. |
| **Commercial/Governmental Requester Audit Unit**<br>**(916) 657-5813** | Questions concerning an audit of your requester account. |
| | All units are available from 8 a.m. - 5 p.m., Monday through Friday (excluding holidays). |

# SURVEY

The Department of Motor Vehicles, Information Services Branch would like your comments about this publication. Please take a moment to answer the following questions by circling one of the numbers for each item, with 1 being the lowest and 5 being the highest, then fold and return to the address indicated on other side of survey:

**1. Did you find this publication informative?**

| VERY INFORMATIVE | | | | NOT INFORMATIVE |
|---|---|---|---|---|
| 5 | 4 | 3 | 2 | 1 |

**2. Did the text answer your questions?**

| ALMOST ALL | | | | ALMOST NONE |
|---|---|---|---|---|
| 5 | 4 | 3 | 2 | 1 |

**3. Was the information easy to understand?**

| VERY EASY | | | | VERY DIFFICULT |
|---|---|---|---|---|
| 5 | 4 | 3 | 2 | 1 |

**4. Is there anything you think should be included or covered better?**

_____

_____

**5. Other comments:**

_____

_____

_____

_____

_____

_____

_____

_____

**(Cut on dotted line)**

STAMP

Department of Motor Vehicles
Policy & Information Privacy Section (PIPS)
MS-H225
P.O. Box 942890
Sacramento CA 94290-0890


THE GREAT SEAL OF THE STATE OF
EUREKA
CALIFORNIA