STATE OF CALIFORNIA
DMV
Department of Motor Vehicles

# Commercial Requester



## Information Handbook

Updated 7/2025

© Copyright, Department of Motor Vehicles 2025. All rights reserved.

This work is protected by U.S. Copyright Law. DMV owns the copyright of this work. Copyright law prohibits the following:

(1) Reproduction of the copyrighted work.
(2) Distribution of copies of the copyrighted work.
(3) Preparation of derivative works based upon the copyrighted work.
(4) Displaying the copyrighted work publicly.
(5) Performing the copyrighted work publicly.

All Requests for permission to make copies of all or any part of this publication should be addressed to:

**Department of Motor Vehicles**
**Legal Office**
**P.O. Box 932382**
**Sacramento, CA 94232-3820**

# Table of Contents


Information Requester Account Program ..... 1
Record Release ..... 2
Permissible Use(s)/Purpose ..... 3
Commercial Requester Accounts Terms and Conditions ..... 4
CHAPTER ONE ..... 7
**COMMERCIAL REQUESTER ACCOUNTS** ..... 7
**SURETY BOND INFORMATION** ..... 9
CHAPTER TWO ..... 10
**CUSTOMER INFORMATION SECURITY REQUIREMENTS** ..... 10
PART I **General Provisions** ..... 10
PART II **Security Requirements** ..... 11
PART III **Additional Security Requirements** ..... 13
**A. Confidential Residence Address Access** ..... 13
**B. Service Providers** ..... 13
**C. Online (Direct) Access – Direct Requester** ..... 14
**D. Online Security Administration** ..... 17
**E. Online (Direct) Access Users** ..... 20
**F. Internet** ..... 21
**G. Batch Processing** ..... 22
PART IV **FREQUENTLY ASKED QUESTIONS** ..... 23
CHAPTER THREE ..... 26
**AUDIT REQUIREMENTS** ..... 26
CHAPTER FOUR ..... 28
**MONTHLY BILLING STATEMENT** ..... 28
**GENERAL QUESTIONS** ..... 29
**GLOSSARY** ..... 30
**FORMS** ..... 32
**CONTACT INFORMATION** ..... 33

# Information Requester Account Program

*Vehicle Code* (VC) §1810.2 authorizes DMV to establish Commercial Requester Accounts (CRAs) and issue requester codes for requesting information.

DMV allows for two types of requesters:

1) Requesters approved to receive information from DMV to fulfill a legitimate business need under one of the following statutes: VC §§1808, 4465, 22851.8, *California Civil Code* §§3067-3075, inclusive, and *Harbors/Navigation Code* §§500-509, inclusive.
2) Requesters who are not approved and request DMV record information on a one-time or occasional basis as authorized under VC §1808.

CRAs are established for applicants who:

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

A requester may be approved for driver's 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).

As a requester, you may request information directly from DMV. Information from DMV can be requested via secure file transfer, online, or indirectly through an approved service provider (see Glossary Section for Service Provider definition).

A requester code may be denied if the proposed use of the information is not related to the requester's legitimate business needs. DMV will immediately cancel the requester code 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 DMV and to protect it from unauthorized access. Additionally, as a Commercial Requester, you are subject to an audit by DMV.

**Information submitted to DMV on an application to obtain a CRA is public record. However, some information contained in these records is classified as confidential, trade secret, or personal under state or federal statutes and is exempt from disclosure**.

# Record Release

DMV may release public record information to any person for an authorized purpose. An authorized business purpose may include, but it is not limited to vehicle/vessel lien sales, underwriting auto insurance policies, and pre-employment screenings. A driver's license and identification (DL/ID) record contains information obtained from an individual's DL/ID application, abstracts of conviction, accidents, and any actions DMV takes against a driver's driving privileges. A vehicle/vessel registration (VR) record contains information relating to the registration of a vehicle or vessel. VC §1808 describes the above as open to public inspection.

Residence addresses are confidential, and information will only be released as authorized by VC §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 VC §§1808.22 or 1808.23. Other confidential information includes physical and mental conditions, controlled substance offenses (VC §1808.5), and social security numbers (VC §1653.5 (f)). Visit **https://leginfo.legislature.ca.gov/faces/home.xhtml** 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 VC §1808.21, signed by the individual whose address is requested VC §1808.22(a).
2. Insurance companies licensed to do business in the State of California when the company, under penalty of perjury, requests the information to obtain 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 VC §§1808.21 and 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 to represent their client in a criminal or civil action, involving the motor vehicle. VC §1808.22(d).
4. Vehicle dealers are 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. VC §1808.23(a)(2).
5. Any person who, under penalty of perjury, requests and uses the information as permitted under *California Civil Code* (CCC) §1798.24(h), if the request specifies that no person will be contacted by mail or otherwise at the address included with the information released VC §1808.23(b).
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. VC §1808.23(a)(1).
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 under the applicable statutes, including but not limited to the following: VC §§22658, 22851, 22851.8, and 22852, CCC §§3067-3074 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 any personal information contained in a motor vehicle record confidential unless the information is requested and used for a "permissible use." A "permissible use" is defined below.

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** – Information received must be used 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** – Information received must be used 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 under an order of a federal, state or local court.

5. **Research and Statistical Reports** – For use in research activities and for use in producing statistical reports so long as the personal information is not published, re-disclosed, or used to contact individuals.

6. I**nsurance 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.

# Commercial Requester Accounts Terms and Conditions

## Commercial Requester Accounts Terms and Conditions

STATE OF CALIFORNIA
DMV
Department of Motor Vehicles

INFORMATION SERVICES BRANCH

**COMMERCIAL REQUESTER ACCOUNT TERMS AND CONDITIONS**

By applying for a Commercial Requester Account to access Department of Motor Vehicles (DMV) information, you, the "Requester," agree to the following terms and conditions, as required under Section H of the Commercial Requester Account Instructions/Application.

DMV reserves the right to modify the following terms and conditions at will.

**A. GENERAL**

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 DMV.

2. Requester and its designees shall only use DMV information for purposes approved by DMV. Any other use is strictly prohibited and will subject Requester and its designees to termination of the account, as well as civil and criminal penalties.

3. Requester agrees to defend, indemnify, and hold harmless DMV and its officers, agents, and employees from any and all claims, actions, damages, or losses, which may be brought or alleged against DMV, its officers, agents, or employees, by reason of the negligent, improper, or unauthorized use or dissemination by Requester or its officers, agents, or employees, of information furnished to Requester by DMV, or by reason of inaccurate information furnished to Requester by DMV, unless Requester can show that DMV was originally furnished accurate information from the reporting source.

4. 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 not specified on the application for a Commercial Requester Account and approved by DMV. Continued storage of information is permissible to comply with federal or state record retention requirements.

5. The person authorized to complete and sign the application on behalf of Requester may be held personally responsible to DMV for any debts and obligations arising under this agreement.

6. Requester shall not represent itself as an agent or employee of DMV. Requester shall not use any DMV trademark or service mark, indicia, acronym, or any substantial similarity thereto, in a manner likely to cause confusion that Requester's services are associated with or are that of DMV.

7. In the event of any breach of the security of Requester's system or database containing the personal information of California residents, Requester shall bear all responsibility for providing notice of the breach to the affected residents, as required by *California Civil Code* (CCC) §1798.82. Requester shall bear all costs associated with providing this notice, and shall also be responsible for providing identity theft prevention services to the affected California residents. These protections include, but are not limited to, providing credit monitoring services for each affected resident for a minimum of one year following the breach of the security of the system maintained by Requester. In addition, Requester agrees to comply with all federal and California state laws, including all of the provisions of the California statutes and Title 13 of the *California Code of Regulations* (CCR).

INF 1233 (REV. 7/2018) **WWW**

8. If DMV or law enforcement contacts Requester about an incident or investigation pertaining to Requester's account or use thereof, Requester shall assist and cooperate with any related investigation. Requester agrees to be held responsible for any misuse of the information by its employees, agents, or parties, to whom the information was entrusted, and to take appropriate corrective actions.

9. Requester shall not sell or transfer ownership of a vehicle or vessel if the information received from DMV records 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.

10. Requester shall notify DMV in writing within ten (l0) days of any changes regarding Requester, including, but not limited to change of address, telephone number, contact person, and closure or sale of business.

**B. SECURITY**

1. Requester shall comply with all DMV security requirements relating to its Commercial Requester Account. Requester understands that 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** (search "Commercial Requester Accounts"). It is the responsibility of Requester to periodically review this website, but no less than once every six (6) months, for any future updates or enhancements to the security requirements. Requester affirms that it has access to the internet to view the website for current security requirements and any requirements that may be updated in the future.

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. FEES**

1. Requesters receiving information directly from 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 the requester account and may include a referral to a collection agency.

**D. DISPUTES**

1. Requester may withhold payment of any disputed charges. A charge is not disputed until Requester provides DMV a written explanation of the disputed charge within thirty (30) days of invoice date. If DMV determines the charge is valid, Requester will be notified and shall pay the outstanding charge within ten (10) days.

2. Requester consents to jurisdiction of California courts and 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 Requester's account shall be adjudicated pursuant to the laws of the State of California.

3. Requester and DMV agree that they shall cooperate to resolve, and negotiate in good faith and in a timely manner, any dispute, controversy, or claim arising out of or relating to the Agreement and/or any Addendum. Requester and DMV further agree to designate promptly one or more authorized representatives with full authority to resolve any such dispute.

## E. INSPECTION OF RECORDS

1. Requester shall keep all records required pursuant to CCR §§350.18(b) (4) and 350.48 at the business address provided to DMV.

2. DMV may perform audits on Requester at DMV's discretion. Requester's place of business shall be available for an electronic or manual audit (of records required to be retained) immediately upon request by DMV or DMV's representative.

3. Requester shall pay reasonable costs in connection with any audit to determine if Requester complies with all of the security requirements and to monitor the requester code usage. Requester shall pay auditing costs within thirty (30) days of DMV's issuance of the invoice to Requester.

4. Requester understands that failure to respond timely to an audit report with findings may result in termination of Requester's account.

## F. SUSPENSIONS/TERMINATION OF ACCOUNT

1. **Suspension for cause with Notice**: If DMV believes a violation of the Commercial Requestor Account Agreement has occurred or is occurring with Requester's account, Requester must participate in any related investigation, and take any necessary corrective action. If Requester refuses to participate in any investigation or take corrective action, DMV shall suspended Requester's account pending the investigation. DMV shall provide written notice prior to any such suspension.

2. **Suspension/Termination for cause without Notice**: DMV may suspend or terminate Requester's account for any violation of the Commercial Requester Account Agreement and/or any Addendum, immediately and without prior notice. If Requester's account is suspended or terminated for violation of the Commercial Requester Account Agreement and/or any Addendum, Requester shall have an opportunity to establish and perform corrective measures to rectify such violation, and prevent future violations. If the corrective measures have the rectified the violation to DMV's satisfaction, DMV, in its discretion, may end the suspension of the account or allow Requestor to reapply for an account.

3. Prior to suspending or terminating the requestor account, DMV shall consider the following:

    a. The nature, extent, and severity of any breach of security, disclosure of information, or dispute, controversy, or claim arising out of or relating to the Agreements and/or any Addendum;

    b. The needs and responsibilities of DMV and law enforcement;

    c. The privacy interests of DMV's customers and their data;

    d. The economic impact of the suspension or termination;

    e. Whether the action is supported by evidence or findings as a result of an investigation or audit;

    f. Whether the action is commensurate or proportional to the findings and circumstances;

    g. Whether Requester can provide a remedy or cure, and the estimated time in which the remedy or cure can be implemented.

    h. Whether Requester has already provided a remedy or cure, and the time in which the remedy or cure was implemented.

4. **Termination without cause**: Either party may terminate the requester account without cause, by giving the other party at least thirty (30) days prior written notice.

# 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 Glossary section for definition of legitimate business need). For further information, see *California Code of Regulations* (CCR) §350.02(m).

2. **How do I apply for a CRA and requester code?**
   You must submit an application for a Commercial Requester code account through the DMV Requester Access Portal at
   **https://www.dmv.ca.gov/portal/vehicle-industry-services/requester-program/.**

3. **Which form(s) do I need to complete for a CRA application?**
   See Forms section for a list of required forms.

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, Service Provider, or Agent (contact the Account Management Unit [AMU] at (916) 657-5564 for additional information).

5. **Is there a fee for the CRA?**
   Yes. Fees to apply for a requester code account are due with the application and renewable every 2 years, the fees are:
   - Basic Record (without residence address) - $50
   - With residence address - $250

   **NOTE:** A surety bond of $50,000 is also required if requesting residence address (see page 10).

6. **How will I know if my application is approved?**
   You will receive a confirmation letter once your application is approved. The approval letter will contain your requester code number(s).

7. **When will my account expire?**
   A CRA is valid for 24 months from the approval date.

8. **Will I be notified to renew my account?**
   AMU will notify account holders approximately 90 days before the account expires by sending a renewal notice to the contact person identified on the account. To avoid any delay in service, ensure that any change to your contact person is reported (see item 12).

9. **Are the fees refundable if I don't qualify for a requester code account?**
   The $50 application fee is non-refundable. If you applied for a CRA account with residence address, and you did not qualify, we will refund the $200 portion of the fee.

**10. How much do the records cost?**

- Each electronic record – Driver's license (DL) or Vehicle Registration (VR) - $2 each.
- Each paper/hard copy – DL and VR records - $5 each.
- Copies of microfilmed records or photos:
  —DL - $20 for each copy.
  —VR - $20 for each year.
- Requests for large volumes or bulk requests - $100 per thousand records, in addition to computer run time and programming fees.

**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 changes to the information provided on the original account application. You must notify DMV of any change(s) to your CRA within 10 working days.

**12. How do I report changes to my account?**

Changes to your account must be made online at **dmv.ca.gov/portal/vehicle-industry-services/requester-program.** Contact the unit listed below for assistance, if needed.

**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 AMU at (916) 657-5564. Allow 60 days for processing.

**IMPORTANT:** Once your account is approved and the requester code(s) is/are assigned, include this number(s) on all correspondence to DMV concerning the specific account.

**14. Do I need a bond to apply for a CRA?**

You will need a surety bond only if you are issued a requester code and have been approved to receive residence address information.

# SURETY BOND INFORMATION

1. **What is the amount of the bond?**
   The surety bond must be $50,000. The bond must be continuous and made payable to the Department of Motor Vehicles.

2. **Where can I obtain a surety bond?**
   The Commercial Requester Account Bond (INF 1132) is available at **dmv.ca.gov**. You should only submit the INF 1132 when requested by DMV after you have been approved to receive residence address information. 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.

3. **What information should the bond contain?**
   The 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.

   Examples are:
   - Sole owner should have the individual's name as well as the doing business as (DBA) on the account.
   - Partnerships should have all partners' individual names and the DBA on the account.
   - Corporations should have the name of the corporation only (if the corporation's name and DBA are identical) or the corporation's name and DBA if different on the account.
   - Limited Liability Corporations should read the Limited Liability Corporation (LLC) and DBA on the account.

   **NOTE:** The bond will be returned to the principal if any information is incorrect or not completed properly.

4. **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. An application is not required to reinstate residence address access when a bond is reestablished and 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; continuance of a Commercial Requester Account is contingent upon Requester's compliance with the updated criteria.

For more information contact the Digital Engagement and Access Unit at (916) 657-5582, to request a copy of "Confidentiality of DMV Records Commercial Requesters".

*Vehicle Code* (VC), Division 1, Article 3, Sections 1800-1825, "Records of the Department" is available at *Leginfo.legislature.ca.gov*.

*VC §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.*

*VC §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.*

*VC §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.*

*California Code of Regulations* (CCR), Title 13, Division 1, Chapter 1, Article 5, "Requesting Information from the Department" is available at: oal.ca.gov.

*California Civil Code* (CCC), 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. Requesters shall maintain the security and integrity of any information they receive and shall maintain records and documents to justify and support proper use of requested information.
3. All Requesters are required to establish and maintain daily logs and source documents (see Chapter Three, item 5) that track the receipt, use, and dissemination of DMV information.
4. The daily log of each request shall be maintained for two years from the date of the request. The log shall be immediately available to DMV upon request. The log format shall provide the following in the order presented:
   - Requester code used to make the request.
   - Date of request.
   - Type of information requested.
   - Points of identification used for the request (for example, driver's license number and date of birth [DOB]).
   - Purpose of the request.
5. The Requester shall notify DMV's Information Policy and Liaison Branch by telephone, at (916) 657-5583 within one business day if fraud or abuse is suspected or confirmed, or the security of the requester code is compromised.
6. A written notification containing all facts shall be prepared by the Requester within three business days and provided to the Information Policy and Liaison Branch (see Contact Information section).
7. The 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.
8. The Requester shall maintain signed INF 1128 forms at the Requester's worksite for at least two years following the deactivation or termination of the authorization and shall be available to DMV upon request.
9. The Requester shall restrict the use and knowledge of requester codes and operational manuals to persons who have signed an INF 1128.
10. The Requester shall maintain and make available to DMV upon request, a current list of names and User IDs of persons authorized to access DMV records, terminal identifiers (termid/netname), and the number of users for each terminal, if applicable.
11. The 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.

12. Access terminals displaying DMV data shall display a “sign-on banner” containing some of the following admonishment in no smaller than 14-point type and in red: “WARNING: Unauthorized access or misuse of data may result in adverse action, including suspension or revocation of the Commercial Requester account and/or criminal prosecution, resulting in a felony or misdemeanor punishable by up to three years imprisonment and a fine not exceeding $100,000, under *California Penal Code* §502 and *Vehicle Code* §1808.46.”
13. The 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).
14. The 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.
15. The 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 INF 1128 other than a DMV approved Service Provider.
16. Requesters are required to implement and maintain adequate physical security for DMV information received (in any format), equipment, and systems that access DMV information.
17. The 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.
18. The 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

### 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 VC §1808.47 and shall comply with additional security requirements contained in this section.
2. Prior to being approved to access and use confidential residence address information, a Requester shall provide the state or federal statute that authorizes 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. The Requester shall not use confidential residence address information obtained for any direct marketing purpose.
4. The Requester shall maintain a log of each request for two years from the date of the request. The log shall be immediately available to DMV upon request. The log format shall provide the following in the order presented:
   - Requester code used to make the request.
   - Date of request.
   - Type of information requested.
   - Points of identification used for the request (for example, driver's license number and date of birth [DOB]).
   - Purpose of the request.

   **NOTE:** An Information Requester Log (INF 2115) is available at **dmv.ca.gov**.
5. Requester shall not obtain or use any information for any purpose other than the purpose approved by DMV.

### B. Service Providers

1. A "Service Provider" is an approved Requester who provides Pass Through connectivity or agent services to another approved End User.
2. Service Providers performing a contracted service (agent) on behalf of another approved Requester shall maintain a log of each request for information for a period of 2 years from the date of the request. The log shall be immediately available to DMV upon request. The log format shall provide the following in the order presented:
   - Date of request.
   - Type of information requested.
   - Whether residence address information was provided.
   - Identify of whom the information was provided.
3. Service Providers providing Pass Through/Reformat Service for DMV approved Requesters shall maintain a log of the request for a period of 5 years from the date of the request. The log shall be immediately available to DMV upon request. The log format shall provide the following in the order presented:

- Date and time of the request.
- End user identity
- Type of information requested (for example, VR, DL, FR and OL).
- Point of identification used for the request (for example, Driver License Number, License Plate number, or Vehicle Identification Number).
- Proposed use as approved by DMV.
- Transaction and information code.

4. Service Provider (Agent) shall provide DMV information only to other approved Requesters and shall include its assigned requester code as part of each inquiry submitted, in a format specified by DMV, in addition to the assigned requester code of the approved requester.
5. Service Provider (Agent) may retain information as required to fulfill its contractual agreement with the approved Requester, or as required by law, as indicated on Agent Authorization Form (INF 03).
6. Service Provider (Agent) shall make available to DMV upon request a copy of the contract between the Service Provider and the approved Requester.
7. Service Provider (Agent) shall notify DMV of any changes, additions and/or deletions regarding its Agent Authorization.
8. Service Providers (Agents) authorized to update DMV information shall comply with the following Update Security Requirements, which may include, but are not limited to:
   - Non-repudiation program application for the electronic update to DMV's database(s).
   - Online (Direct) Security Administration and electronic validation programs.
   - Restrict transaction types as necessary to ensure the user is authorized for updates.
   - Encryption, a Virtual Private Network.
9. 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's 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. Online (Direct) Access – Direct Requester

A Service Provider requesting direct online access to DMV database is required to have a Special Permit. Those Service Providers not having a Special Permit may request DMV information through a Secure File Transfer (SFT) or another Service Provider approved by DMV and has been issued a Special Permit.

1. A "Special Permit" is a signed agreement between DMV and a Service Provider authorizing online (direct) access to the DMV's database. In addition to any other applicable section, a Special Permit Holder shall comply with all additional online security requirements contained herein.
2. The Special Permit Holder shall maintain the security and integrity of DMV information and the online information service system.
3. The 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 the Special Permit Holder's computer system shall be a termination point in the communications network as approved by DMV.
5. No terminal or system shall act as an intermediate communications node for other remote systems.

6. The Special Permit Holder shall submit, for DMV approval, the current Special Permit Holder's Network Topology containing functional system descriptions, all terminals (if applicable) and a security component narrative that describes how each security requirement is to be met by the Special Permit Holder, Network Narrative, and the DMV Information Security Agreement (DISA). If employing more than one type of system, documentation shall be supplied for each type. A Network Topology and the security component narrative shall be supplied:
   - Upon the Special Permit Holder's initial online information service request.
   - A minimum of 30 days, in advance, for DMV's review of any changes being made in hardware or software systems that affect the Special Permit Holder/End User communication access to DMV's database(s).
7. The 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 10-15 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. The Special Permit Holder shall maintain an electronic file of the User ID, requester code, date and time of every occurrence where the Special Permit Holder has automatically terminated an access due to non-use within a 10-15 minute time period. These records shall be kept for two years from the date of the access termination and shall be available to DMV upon request.
9. The 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. The 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 unauthorized access to DMV information.
11. The Special Permit Holder shall terminate access to a Requester and shall notify DMV's Digital Engagement and Access Unit (see Contact Information Section) within one working day when the Requester refuses compliance with or violates any security requirement.
12. The Special Permit Holder shall electronically log each transaction transmitted to a Requester. Information electronically logged shall include:
    - Transaction code.
    - Information code.
    - Requester's requester code.
    - Record identifiers (for example, driver's license number, vehicle license plate number, vehicle identification number [VIN]).
    - Individual User ID.
    - The date and time of the transaction.
    - Date record received from DMV.
    - Requester's terminal location.
    - 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 2 years from the date of the transaction. The Special Permit Holder shall be capable of selectively listing inquiry transactions based on specific criteria, defined by DMV, including, but not limited to, a Requester's requester code and User ID. A printed report or electronic file shall be submitted to DMV upon request. The 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 the 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 functionality defined in Part III, D. Any deviations must have advanced written approval by DMV.
14. The 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. The Special Permit Holder shall not have a compiler or an assembler connected to the production computer accessing DMV information.
16. The 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 the Special Permit Holder. Additional test records will be created for the Special Permit Holder upon written request. Requests to use the test database(s) must be approved in advance by contacting DMV's Digital Engagement and Access Unit (see Contact Information Section).
18. The Special Permit Holder shall install and maintain cost for establishing online 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 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.
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 online 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. Online 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 online access or access and update to DMV files for an authorized Requester. Special Permit Holder may act as both a Service Provider and an End User provided a clear separation between the functions and separate requester codes are utilized. Please note the following:
    - An organizational chart that identifies a clear separation of the Service Provider and Requester functions is submitted.
    - Service Provider and the Requester utilize separate requester codes on all transactions.
    - All Service Provider and Requester requirements specified apply to the respective functions.

- Security administration configurations and system design for combined Service Provider/Requester systems are approved by DMV.
- Establish independent system hardware for the Service Provider and Requester functions.
- Company owners, partners, or corporate principal officers shall not serve as Access Control or Review Administrator.
- Access Control Administrator duties and Review Administrator duties are performed by different individuals.

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

## D. Online Security Administration

**1. Security Administration**

Security administration is the responsibility of the Service Provider when providing Pass Through services. This function includes both Access Control Administrator and Review Security Administrator. The Service Provider shall ensure that all requirements of security administration are met. The Service Provider 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 be delegated to the Requester client with prior written approval from DMV. If these functions are delegated to the Requester, the following required steps must be completed.

- A Service Provider shall submit a written request for approval to DMV's Digital Engagement and Access Unit (see Contact Information Section) prior to delegating Access Control Administration to an approved Requester. The written request shall include:
  —A statement that the Requester will be responsible for the Access Control Administration functions instead of the Service Provider.
  —A description of the business purpose for the request.
  —The name and title of the individual designated as the Access Control Administrator.
  —The name and title of the individual designated as the Review Security Administrator.
  —Signature of Requester authorized to sign for the Commercial Requester Account.
  —An approval line for the signature of the Service Provider and the signature of the Policy and Liaison Branch Chief for concurrence and approval.
  —A Network Topology and security narrative that complies with all of the security, technical, and programming requirements.

**3. Access Control Administrator**

- 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 (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.
  —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 identity. Authorization shall be controlled by software that limits the functions a particular user can perform.

- 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.
- 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.5. – User ID/Password Standards**).
- 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 (the encryption cannot be removed from the password).
- An electronic file containing User ID, date, and time for each occurrence of a password change shall be maintained.
- 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 5 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.
- 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.
- 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 by DMV in advance.
- 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:
  —The holder of the User ID no longer requires access to DMV information.
  —The holder of the User ID authorized for DMV record information access –leaves the employ of Special Permit Holder or Requester.
  —The holder of the User ID is suspected of unauthorized disclosure or misuse of DMV information.
  —The holder of the User ID does not comply with DMV's information security requirements.
  —Requester access is terminated. The Access Control Administrator shall revoke the User ID of all Requester employees utilizing the Online Information Service.
- 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 the Terms and Conditions.
- Individual's User ID will be assigned and controlled by the Access Control Administrator. The Access Control Administrator shall require each individual to utilize the user authentication method to initiate each session logon as defined in Section D.3. Before an inquiry transaction may be initiated, the individual's User ID must be validated and accepted by the

security administration computer system.

- The Access Control Administrator shall maintain an electronic file of all individuals accessing DMV information. Each electronic file shall include:
  —The date access was initially granted.
  —Business name, address, and telephone number.
  —Requester code.
  —Individual's name and User ID.
  —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 2-year history of any and all changes to the information shall be kept for all individuals with current online information access. For inactive users, this information shall be retained for two years from the date online information access was terminated.

**4. Review Security Administration**

- 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.
- 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 five consecutive unsuccessful logon attempts.
- The Review Administrator shall notify DMV in writing within 3 working days of any individual who submits 3 consecutive unauthorized transactions. Mail or email the notification to the DMV's Information Policy and Liaison Branch (see Contact Information Section).
- The Review Administrator shall notify the Special Permit Holder within one working day of any of the occurrences noted by the Access Control Administrator defined in **Section D.3**. 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.
- The Review Administrator shall monitor the online 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.
  —Complete log information has been kept for each unauthorized inquiry transaction attempt.
  —Complete access control information has been kept for each completed transaction.
  —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 **not**:
    ○ Authorized by DMV.
    ○ Valid for the user initiating the transaction.
    ○ Valid for a particular transaction.
    ○ Valid for a particular Requester device identifier (wrong terminal/communication line).
- The Review Administrator shall check for patterns that might indicate unauthorized attempts to gain access to DMV files. The Review Administrator shall investigate suspected unauthorized access attempts should unauthorized access attempts be confirmed.

- The Review Administrator shall immediately alert DMV's Information Policy and Liaison Branch by telephone at (916) 657-5583, with a written follow-up submitted to DMV's Digital Engagement and Access Unit within one working day (see Contact Information Section).
- 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.

**5. User ID/Password Standards**

- Password authentication requires a unique identification component (User ID) assigned by Requester and a confidential password component. Both components are required for authentication.
- Assignment of User IDs and default passwords must be accomplished using a secure process, (for example, do not email in clear text).
- DMV User ID requirements:
  - —User ID must be unique to each individual and not assigned to groups or job locations.
  - —User IDs shall be revoked after 5 consecutive unsuccessful logon attempts. Reauthorizing the User ID requires verification of the user's identity.
  - —"Default" passwords, known only to the user, may be used for the purpose of resetting the account. Default passwords may not be used to conduct business.
- Password requirements:
  - —Passwords must be validated by the system against the User ID for each logon to the system.
  - —The owner of the User ID shall choose passwords.
  - —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.
  - —Passwords are required to be at least 15 characters in length, include an upper/lower case, numeric, and a special character.
  - —Passwords must consist of both alpha and numeric characters.
  - —Passwords shall not utilize symbols or punctuation marks (#, %, !, etc.).
  - —Passwords must expire in 90 days or less.
  - —Passwords shall not be displayed in a readable manner on the screen when keyed.
  - —Users are required to obtain administrator authorization to change their password a second time.
  - —The system shall prevent the user from re-using the password within 12 password history iterations.
  - —Passwords stored in the program must be encrypted using Data Encryption Standard, or equal/better, one-way-only encryption.
  - —Passwords must never be written down or displayed in plain text. This requirement can be enforced by written policy.
  - —System-level passwords (for example, root, enable, network, application, local, and enterprise-level administration) are required to be changed at least every 90 days.

## E. Online (Direct) Access Users

1. A Requester Account User who has online (direct) access to DMV information through an approved Service Provider shall, in addition to any other applicable sections, comply with all security requirements contained in this section.

2. Login 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 the User's ID for each authorized individual user 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 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 (for example, their name, initials, family members, etc.).
3. Passwords shall be changed at least every 90 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 by close of business day upon termination of 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 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.
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 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.

## 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 Department of Motor Vehicles Information Security Agreement (DMV ISA).

## G. Batch Processing

1. When use of Secure File Transfer (SFT) based technologies is included in any portion of the information-processing environment, all Requesters shall comply with any requirements specified in the SFT User Manual. Contact the Automation Delivery Unit at (916) 657-5582 to have a copy of the 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. Demilitarized Zone (DMZ) configurations do not meet this requirement.
3. SFT batch customers must change their SFT User ID Password at least every 60 days.
4. In addition, passwords:
   - Must be at least 9 characters long.
   - Must have at least 1 alpha character and 1 upper case letter.
   - Must have at least 1 numeric character(s).
   - Must have a least 1 special character (s).
   - Will be locked out of the system after 3 erroneous password attempts.
   - Can be changed at any time.
5. Minimum hardware/software requirements are identified in the SFT User Manual.
6. As technology improves/changes, additional security concerns and changes may be required.
7. Requesters will be required to submit a completed SFT Electronic Data Transfer application prior to conversion of batch program(s) output.
8. Input files are processed Monday through Friday, excluding DMV non-business days (holidays, weekends, etc.). The DMV holiday schedule is available at **dmv.ca.gov** by searching "state holidays" or contacting the Automation Delivery Unit at (916) 657-5582.
9. The daily production schedule begins at 4:30 p.m. (Pacific Standard Time). Input files sent by this time will be available the next business day, by 7:00 a.m. (Pacific Standard Time).
10. All SFT connections must meet, at a minimum, the following requirements in order to protect the integrity and confidentiality of DMV data. These requirements apply to all SFT connections, including router-to-router, lan-to-lan, and client connections.
11. Operating System (OS) Requirements: Windows, Mac, Linux/UNIX, Mainframe The client/web browser will determine the specifics of the OS.
12. Web Brower Requirements: Internet Explorer® 6.0 SP1 and higher, Firefox® 2.x and 3.x.
13. Permission Requirements for Web Browser Ability to save cookies (session management)
14. Desktop Anti-virus Protection: Up-to-date anti-virus protection software on each client station.
15. All hosts that will transfer data to/from DMV must exist behind an internal firewall and the system must be protected on a trusted network located in the United States. Hosts in a DMZ configuration do not meet this requirement. Firewall and network configuration changes may affect your SFT connection. Technical staff from DMV's Electronic Production Process Unit may be able to assist.

# PART IV

## FREQUENTLY ASKED QUESTIONS

1. **What are the available methods to receive information from DMV?**
   Information can be received either directly from DMV or through a DMV approved Service Provider. For a current list of approved Service Providers, visit **dmv.ca.gov.**

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 DMV. (See Glossary Section 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 the purpose for which it was requested and as long as it is required.

   **IMPORTANT**: Residence addresses information received from DMV records may not be used for any direct marketing or solicitation for the purchase of any consumer product or service (VC §1808.23(b)).

4. **If I am a consumer reporting agency as defined in 15 USCS 1681(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 verify 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's license or identification number, physical characteristics, etc., by shredding, erasing, or modifying the personal information to make it unreadable or undecipherable, as provided in *California Civil Code* §§1798.80, 1798.81, and 1798.82.

6. **If someone is 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 DMV, the person shall require the agent to take all steps necessary to ensure the 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. Which DMV forms must be signed by someone acting as my agent or by my employees?**

An Information Security Statement (INF 1128) form 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. VC §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 at the requester's worksite and available to DMV's auditors.

**10. Do I need to have anyone in charge of securing this information?**

Yes. The Requester is responsible for ensuring someone is in charge of maintaining the security of DMV information. The Requester must be able to provide the name, title, and telephone number of that person upon request.

**11. What other security requirements must I or my employees be aware of if accessing DMV information by computer?**

- Remember, account holders are personally responsible for all activity occurring under their User ID while signed on to the DMV computer.
- Do not write passwords down or tell your password to anyone. Passwords are not to be shared among individuals or groups.
- Always log off the terminal each time the terminal is left unattended.
- Passwords should be changed at least every 90 days or less, to help prevent unauthorized access.
- DMV information should only be requested and used for the purpose for which it was approved.
- Do not have your terminal screen visible to anyone that is not authorized to view the information.
- DMV information must be properly destroyed when legitimate business need has ended.
- 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.
- Printed records, and any records stored to any electronic media (diskette, hard drive etc.), must be protected from unauthorized access and viewing.
- 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:

- Requester code.

- Date of request.
- Name of the subject of request.
- Information requested (Driver's License, Vehicle Identification Number (VIN)/Hull Identification Number (HIN), and Vehicle/Vessel Plate Number).
- Reason or purpose for the request and supporting documentation.
- Cross-reference to the corresponding supporting documentation (for example, file/case #, account #, inventory/control #, etc.)
- **NOTE:** An Information Requester Log (INF 2115) form is available at **dmv.ca.gov**.

**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 in accordance with CCR §350.48.

**15. Whom should I notify if I suspect fraud or misuse of DMV record?**

If fraud or misuse is suspected or confirmed, you must notify DMV's Information Policy and Liaison Branch (IPLB) at (916) 657-5583, within one business day of discovery. A written notification containing all facts must be prepared by the requester within three business days and submitted to IPLB by mail or email:

Department of Motor Vehicles
Information Policy and Liaison Branch, MS H225
P.O. Box 942890
Sacramento, CA 94290-0890
cpdisbpips@dmv.ca.gov

**IMPORTANT**: Failure to keep complete logs of requested information and to maintain a signed INF 1128 for each person authorized to access DMV information remain the most common noncompliance finding by DMV auditors. To avoid suspension of your account, please ensure you maintain accurate logs and signed INF 1128 for each authorized employee. For logging purposes, you may use INF 2115. INF 1128 must be re-certified annually.

# CHAPTER THREE
## AUDIT REQUIREMENTS

The DMV Audits Office, Commercial/Government Requester Audit (CGRA) Unit audits Commercial Requesters to ensure compliance with the requirements of *Vehicle Code* (VC), *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 (online, hardcopy, secure file transfer, etc.) or the type of information that the requester is authorized to receive (basic, residence address, mailing address or residence address with post notification).

   Certain conditions may warrant an unannounced audit, however, in most cases DMV will contact the requester by email approximately 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 selection criteria determined by the management of the DMV Audits Office, CGRA Unit.

3. **What happens during the audit process?**
   The audit consists of:

   - An entrance conference to explain the audit process.
   - Testing and review of supporting documentation.
   - An exit conference to inform you of any findings.
   - A written draft audit report.
   - Auditee (requester) submits a written and signed response to findings (if any) or includes a detail of corrective action and implementation date.
   - A written final audit report.

   Typical audits take 8 to 10 weeks to complete, however, some may require additional time.

4. **What do I need for the audit?**
   The auditors will review, but not limit the audit to, the following:

   - Supporting documentation to show evidence of proper use.
   - Required logs (see page 15.)
   - Information Security Statements (INF 1128).
   - Listing of authorized employees to request information.
   - Listing of authorized employees who were terminated.
   - Billings or invoices from your Service Provider.

   The supporting documentation must be made available for the audit and kept at the physical place of business listed on the Commercial Requester Account Application (INF 1106) form and Commercial Requester Account Branch Location Requester Code(s) Application (INF 1106BL) form 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:

   - **Insurance companies** provide policy numbers, accident reports, Traffic Accident Report (SR-1) information or insurance quotes.

   - **Law offices** supply a client information sheet, retainer agreement, accident report and court case number.
   - **Private investigators** provide case names, file numbers, client information and reports.
   - **Registration services** supply information related to the transaction processed, such as fees collected, method of payment, date fees collected, and cost to client.
   - **Dealers** pull their dealer jacket, purchase/lease agreement/odometer disclosure statement, release of liability, title, registration or a bill of sale.
   - **Towing companies** provide towing and lien sale data.
   - **Auto auctions** provide stock/inventory numbers, reports of sale, and buyer/seller information.

6. **What happens after the audit?**
   Once the audit is completed and reviewed by management, an audit report will be 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.

   Audits with findings (non-compliance with VC, CCR, and the Terms and Conditions of the Commercial Requester Account or other applicable statutes) are subject to final determination by Information Policy and Liaison Branch management for adverse or corrective action (re-audit, monitoring, referral to legal office or referral to investigation).

7. **Can DMV take any other actions?**
   If an audit discloses a violation of any state/federal laws or any provisions of Title 13 of the CCR, 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 VC §§1808.45 and 1808.46 and Title 13 of the CCR.

8. **Is there anything else I should know about the audit?**
   If the audit reveals a violation(s) of VC §1808.22 through 1808.47 and/or a violation(s) listed under CCR §350.52 the requester may be subject to administrative, civil, or criminal action.

9. **If my account is terminated either voluntarily or involuntarily, what should I do?**
   Whenever an account is terminated pursuant to CCR §350.16, DMV may require the holder to surrender all information and records retained pursuant to CCR §350.18(b)(4) and (5) and CCR §350.48, 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.

# CHAPTER FOUR

## MONTHLY BILLING STATEMENT

1. **When will I be billed?**
   When a bill reaches $50 or every 3 months, an invoice will be delivered no later than the 10th of the month. If you obtain information through a Service Provider, 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?**
   Online payment option is available at
   **dmv.ca.gov/portal/vehicle-industry-services/requester-program**.

4. **What happens if I do not pay my bill on time?**
   Failure to pay your bill could result in the cancellation of your requesting privileges and may include a referral to a collection agency or collection against your bond. Pursuant to CCR §350.46(a), your requester code will be revoked if any amount remains unpaid 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 Account Management Unit (AMU) in writing within 30 days of the invoice date (see Contact Information Section).

6. **How can I report changes to my billing address?**
   You may use the Requester Access Portal to make changes to your billing address.

7. **Who can I call if I have questions about my bill?**
   You can call the AMU at (916) 657-6474

# GENERAL QUESTIONS

### ATTORNEYS FOR MOTOR VEHICLE RELATED INCIDENTS

**Q. I am an attorney representing a client in a motor vehicle related incident pursuant to *Vehicle Code* (VC) §1808.22. May I release the residence address to an attorney service or licensed private investigator to perform service of process?**

A. Yes, the attorney service or licensed private investigator would become your agent. A signed Information Security Statement, (INF 1128) form, 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.

### BRANCH LOCATIONS

**Q. What is a branch location?**

A. An offshoot, lateral extension, or division with a separate physical location but under the same corporate number and ownership.

### SHARING REQUESTER CODE

**Q. I am an approved End User whose requester code does not permit access to residence address information and am authorized to perform background or pre-employment screenings. My client is an approved account holder whose requester code permits access to residence address information. Can I use their requester code?**

A. No. An account holder may not share their requester code with anyone except an employee, an agent, or a Service Provider who has signed an INF 1128.

### BACKGROUND CHECKS/PRE-EMPLOYMENT SCREENING

**Q. Is a background check or pre-employment screening considered reselling DMV information?**

A. No. A DMV record may be part of a background check or pre-employment screening as part of a compilation of other information (for example, employment or credit history, etc.). If the DMV record is the sole document used to perform the background check or pre-employment screening, this constitutes a resale and is expressly prohibited.

### SERVICE PROVIDER

**Q. Is a person required to have an account with DMV to get record information through a department-approved Service Provider?**

A. Yes. A DMV-approved Service Provider is only authorized to release DMV record information to an authorized End User with requester account.

# GLOSSARY

**Agent**
As authorized by DMV, a person or entity who is authorized by a DMV-approved requester to access, receive, or use DMV record information on behalf of its client who is a DMV-approved requester.

**Account Contact Person**
The contact person must be a firm employee familiar with the account who has 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**
A commercial entity approved by DMV and issued a requester code to purchase information from DMV.

**Consumer Reporting Agency (Fair Credit Reporting Act 15 U.S.C. §1681)**
Any person who, 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 to furnish 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**
Any requester account holder for whose use information is requested from DMV records either directly or through a Service Provider/agent.

**Fair Credit Reporting Act 15 U.S.C. § 1681**
A federal statute enacted to protect individuals from inaccurate or arbitrary information documented in consumer reports.

**Legitimate Business Need**
An authorized purpose for requesting, obtaining, disclosing or using information contained in a DMV 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 of a type subject to registration under the *Vehicle Code*.

**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.

**Public Record**
*Vehicle Code* §1808 and the Public Records Act (*California Government Code* §7920) provides that information collected by DMV 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 and numbers assigned by DMV to identify a requester.

**Service Provider**
A requester account holder who has been authorized by DMV to provide a Pass Through service to a DMV-approved requester. For information regarding Service Providers, contact the Account Management Unit at (916) 657-5564.

# FORMS

The following forms are provided in the Commercial Requester Account (CRA) Instructions/Application (INF 1133) packet or the Commercial Requester Account (CRA) Service Provider Application (INF 1133V) packet. All forms are available at **dmv.ca.gov**.

**INF 1106 Commercial Requester Account Application**
Complete this form if you will be using DMV record information for your own business use (for 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 Commercial Requester Account Branch Location Requester Code(s) Application**
Account holders with multiple branch locations needing different requester codes must complete this form.

**INF 1106V Commercial Requester Account Service Provider Application**
Complete this form if you will be accessing DMV record information to perform a legitimate business service on behalf of another CRA applicant (for example, pass thru/reformat [Service Provider] 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 Information Security Statement**
This form must be signed annually by any individual who has access to information received from DMV. It must be retained at the account holder's worksite. Do not send to DMV.

**INF 1132 Commercial Requester Account Bond**
This form will be mailed to you once you have been approved for residence address access.

**INF 1184 Information Services Certification of Agency**
Any vehicle dealer/manufacturer agent requesting residence address information 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 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 send to DMV.

**INF 03 Information Services Program Agent Authorization Form**
This form must be completed and signed by each approved requester using a Service Provider as an agent when residence address information is being requested. This form is not necessary when the Service Provider will only be providing Pass Through connectivity (non-agent) service.

# CONTACT INFORMATION

All units are available from 8 a.m. - 5 p.m., Monday through Friday (excluding holidays).

| | |
|---|---|
| **Requester Account Questions**<br>(Account and Billing Inquiries) | **Account Management Unit – H221**<br>PO Box 944231<br>Sacramento, CA 94244-2310<br><br>Government and Commercial Requester Account Inquiries<br>(916) 657-5564<br>cpdapu@dmv.ca.gov<br><br>Billing Inquiries<br>(916) 657-6474<br>cpdabis@dmv.ca.gov |
| **Electronic Access Methods**<br>(Secure File Transfer and Online Direct Access) | **Automation Delivery and Digital Engagement & Access– R390**<br>PO Box 942890<br>(916) 657-5582<br>cpdadu@dmv.ca.gov |
| **Policy/Information Privacy**<br>(Policies regarding DMV record release and/or uses) | **Information Policy and Liaison Branch – H225**<br>PO Box 942890<br>Sacramento, CA 94290-0890<br>(916) 657-5583<br>cpdisbpips@dmv.ca.gov |
| **Audits**<br>(Questions concerning Requester Account audits) | **Commercial/Governmental Requester Audit Unit F121**<br>PO Box 932328<br>Sacramento, CA 94232-3280<br>(916) 657- 6480 |