DMV Information—Use Criteria

**Purpose:** To assist the customer in completing parts eight and nine of the Information Use Application form US 531A/AR.

**User Qualification**
- Valid user — proper ID/Business or Professional License; authorized by statute, rule, or regulation
- Valid use of information — allowed under state/federal laws
- Completed and approved DMV Information Use Application (US 531A/AR)

**Password Codes/Authorized User Passwords and Codes**
- Will be assigned by DMV/Information Technologies Systems Administration
- Access codes issued to user for access and billing
- Authorized users have distinct access codes

**Information/File Security**
- User should keep all information in a secure area or locked cabinet
- Access to these areas or files must be limited by physical security measures
- Propose an audit/management control over access and dissemination of requested information

**Computer Security**
- Computer terminals or personal computers must be in physically secure area
- Computerized storage will only be allowed as expressly written in an information use agreement, addendum, or contract and
- Storage media and devices must be physically secure and/or secured by appropriate computerized security measures (acceptable industry standards)
- For automated interfaces/electronic extraction and storage of data, if applicable, address how you plan to secure the following items:
  - Records, files and systems
  - Names and addresses of data extraction method and software creator/vendors
  - Network diagrams and descriptions of data extraction methods and software
  - Descriptions of system support processes including backup methods and frequencies

**User Logs**
- Users must keep an access log of authorized users, dates and times accessed, purpose accessed, subject of inquiry, user making access, and a copy of the information use agreement,
- For driver history information, users must keep a valid signed authorization to act as an agent for the data subject, as required by statute, rule, or regulation.

**Secondary Dissemination Logs**
All persons or entities receiving a copy (physical, computerized or photocopy) of information from the user should be listed in a chronological log stating what information was released, in what format, and for what purpose

**Rule and Regulation Compliance**
The Department of Motor Vehicles (DMV) may audit a user's compliance with the stated rules and regulations concerning DMV information.

All users are subject to records review and on-site audits. Examples of why an audit may be conducted are as follows:
- Complaints received concerning information use
- Number of records accessed in a given timeframe
- Random review/audit by DMV
- Cyclical review (yearly, semi-annually, monthly)