MINNESOTA DEPARTMENT OF PUBLIC SAFETY
DRIVER AND VEHICLE SERVICES

RECORDS ACCESS AGREEMENT
Government Agency

FEIN _____

This agreement is between the State of Minnesota, acting through its **Department of Public Safety** (hereinafter "STATE")

and _____

a representative of _____

located at _____ (hereinafter "GOVERNMENT BUSINESS PARTNER").

If you are a private law firm acting as a city/county attorney, please identify the city/county the GOVERNMENT BUSINESS PARTNER represents. You must also provide documentation that the GOVERNMENT BUSINESS PARTNER is authorized to work on behalf of the city/county referenced.

City/County Representing _____

I understand by signing this document I agree to the following terms and conditions to gain access to the STATE's Driver and Vehicle Services Division (hereinafter "DVS") information system for a GOVERNMENT BUSINESS PARTNER and only for the use(s) described in the Government Business Partner Intended Use Statement.

1. Access to the DVS information system is restricted to the GOVERNMENT BUSINESS PARTNER's authorized users who need access to perform their job duties.

2. The GOVERNMENT BUSINESS PARTNER will provide the STATE with specific use(s) of DVS data by the GOVERNMENT BUSINESS PARTNER's authorized users in number 17 of this agreement which is entitled *Government Business Partner Intended Use Statement.* Based on the information provided, the STATE will determine the appropriate access allowed by statute and applicable laws. DVS data obtained by the GOVERNMENT BUSINESS PARTNER will only be used for the purposes approved in number 17 of this agreement.

3. The GOVERNMENT BUSINESS PARTNER will not use DVS data for personal or non-business purposes. Any such use is in violation of state and federal laws.

4. The GOVERNMENT BUSINESS PARTNER is responsible for training all authorized users on the proper use and dissemination of DVS data. Training will be done in compliance with DVS data privacy training materials. The training material attestation (*Security and Confidentiality of Data and Records Access Attestation*) must be retained by the GOVERNMENT BUSINESS PARTNER and submitted to the STATE upon request. (See **Exhibit A**.)

5. The GOVERNMENT BUSINESS PARTNER will require each authorized user who has a business need to access the DVS data to sign an *Authorized User Records Access Agreement* regarding usage and dissemination of DVS data. The *Authorized User Records Access Agreement* is maintained by the GOVERNMENT BUSINESS PARTNER and submitted to the STATE upon request.

6. The GOVERNMENT BUSINESS PARTNER will disable an authorized user's access within three (3) calendar days of an assignment change or when no longer employed.

7. The GOVERNMENT BUSINESS PARTNER understands each authorized user is assigned a unique username (user-specific email address that must contain the authorized user's personal name or identifying initials), and the authorized user's password information will not be shared with anyone, including other employees or their supervisors.

8. The GOVERNMENT BUSINESS PARTNER understands that improper use or dissemination of DVS data will result in **disciplinary action** under Minnesota Statutes, section 171.12, subdivision 1a(b). Criminal and civil penalties under both state and federal laws may also apply.

9. **Information Security**

   The GOVERNMENT BUSINESS PARTNER is required to secure and protect the DVS data requested in this agreement. The appointed Administrator must review and *initial* next to each of the following to indicate compliance with the information security requirements.

   Data Storage

   _____ The GOVERNMENT BUSINESS PARTNER will securely store electronic and/or paper copies of GOVERNMENT BUSINESS PARTNER records, including supporting documentation for every record viewed.

   Security Software

   _____ The GOVERNMENT BUSINESS PARTNER will have a security software program which may be used in conjunction with a firewall, utilized on devices used to access DVS data and where DVS data is stored.

   Authentication Method

   _____ Authorized users of the GOVERNMENT BUSINESS PARTNER will each have secure individual login credentials on devices used to access DVS data and where DVS data is stored.

   Supporting Documentation

   _____ The GOVERNMENT BUSINESS PARTNER must record in the DVS information system the approved business reason for each record viewed. The Administrator acknowledges that the GOVERNMENT BUSINESS PARTNER will retain supporting documentation for at least five (5) years from the date of the record view and the supporting documentation must be presented to the STATE upon request. The Administrator also acknowledges that they will notify each authorized user of this requirement.

10. **Certification**

    The GOVERNMENT BUSINESS PARTNER or an authorized user must not use noncompliant (credential that does not meet the REAL ID Act) driver's license or identification card data for civil immigration enforcement purposes or disclose the data to a state or federal government entity that primarily enforces immigration law or to any employee or agent of any such government entity. If the GOVERNMENT BUSINESS PARTNER or an authorized user violates this certification, they may be liable in a civil action brought under Minnesota Statutes, section 13.08, may be subject to criminal penalties under Minnesota Statutes, section 13.09, and may have subsequent requests for noncompliant driver's license or identification card data be denied by the Commissioner.

11. **Report of Misuse**

    All incidents of misuse, or suspected misuse, by GOVERNMENT BUSINESS PARTNER authorized users must be reported to DVS immediately. DVS will examine each incident for validity and forward any substantiated report of misuse for further investigation to the GOVERNMENT BUSINESS PARTNER and/or law enforcement. Failure to report confirmed or suspected misuse may result in suspension or cancellation of the GOVERNMENT BUSINESS PARTNER's access.

12. **Liability**

To the extent provided by law, the GOVERNMENT BUSINESS PARTNER will indemnify, save, and hold the STATE, its agents, and its employees harmless from any claims or causes of action, including attorney's fees incurred by the STATE, arising from the performance of this agreement by the GOVERNMENT BUSINESS PARTNER or the GOVERNMENT BUSINESS PARTNER's authorized users. This clause will not be construed to bar any legal remedies the GOVERNMENT BUSINESS PARTNER may have for the STATE's failure to fulfill its obligations under this agreement.

13. **Government Data Practices**

The GOVERNMENT BUSINESS PARTNER and the STATE must comply with the Minnesota Government Data Practices Act, Minnesota Statutes Chapter 13, and 18 U.S.C. section 2721, as they apply to all data provided by the STATE under this agreement, and as it applies to all data created, collected, received, stored, used, maintained, or disseminated by the GOVERNMENT BUSINESS PARTNER under this agreement. The civil remedies of Minnesota Statutes, sections 13.08 and 13.09, and 18 U.S.C. section 2721 apply to the dissemination of the data referred to in this clause by either the GOVERNMENT BUSINESS PARTNER or the STATE. (See **Exhibit B** and **Exhibit C**.)

14. **Audits**

The STATE maintains an electronic log of data accessed through the DVS information system. This electronic log includes, in part, the username, date, time, IP address, and the data searched. The GOVERNMENT BUSINESS PARTNER must maintain a way to verify work-related searches. This record must be maintained for at least five (5) years from the date of the search and must be presented to the STATE upon request.

Inspection of Records: The GOVERNMENT BUSINESS PARTNER's place of business shall be available within a reasonable period of time for an electronic or manual audit of records upon request from the STATE or its representative. The GOVERNMENT BUSINESS PARTNER understands that failure to respond to an audit report request with findings may result in suspension or cancellation of the GOVERNMENT BUSINESS PARTNER's access.

Audits will be conducted at the GOVERNMENT BUSINESS PARTNER's expense.

15. **Termination**

The STATE or the GOVERNMENT BUSINESS PARTNER may terminate this agreement at any time, with or without cause, upon written notice to the other party.

16. **Delegation of Data Administrator**

The Administrator is the only person from whom DVS will accept changes.

Administrator Responsibilities

Administrator responsibilities include all areas of access management for all GOVERNMENT BUSINESS PARTNER's authorized users, including:

Before Authorizing Access

- Obtain a signed *Authorized User Records Access Agreement*;
- Review with the authorized user, *Policy 125-1000 Security and Confidentiality of Data and Records*. After review, have the authorized user sign the *Security and Confidentiality of Data and Records Access Attestation*;
    - As part of the policy review, the administrator must review *Frequently Asked Questions - Accessing Driver and Vehicle Services Data and Records* with the authorized user;
- Verify the identity of the authorized user via a current state issued identification (ID) or driver license (DL);

- Provide the authorized user with training on the proper use and dissemination of DVS data; and
- Notify authorized users at the GOVERNMENT BUSINESS PARTNER the approved business reason for access, as specified in this agreement.

Other Responsibilities

- Provide the authorized user with the means for access;
- Assign appropriate level of access to authorized users;
- Remove access within three (3) calendar days when an authorized user no longer needs access due to an assignment change or is no longer employed by the GOVERNMENT BUSINESS PARTNER;
- Ensure authorized users receive, review, and understand DVS email updates;
- Maintain the initial and annual policy attestation documentation of authorized users for five years;
- When needed, provide the authorized users with training on the proper use and dissemination of DVS data; and
- Cooperate with DVS on any audits concerning the access to the DVS information system.

At Least Annually

- Review with the authorized user, *Policy 125-1000 Security and Confidentiality of Data and Records*. After review, have the authorized user sign the *Security and Confidentiality of Data and Records Access Attestation*.
    - As part of the policy review, the administrator must review *Frequently Asked Questions - Accessing Driver and Vehicle Services Data and Records* with the authorized user.

Please attach a legible copy of your current state issued driver license (DL) or identification (ID) card to verify your identity for access. You are not legally required to provide this document. However, without a copy of your DL or ID card, DVS is unable to provide you with access to the DVS information system. The information may be accessed by internal staff and external auditors.

Administrator's Legal Name (please print or type)

Administrator's User Specific Email Address

Administrator's Phone Number

Administrator Attestation

I attest that I have read and understand my responsibilities as the Administrator.

Administrator's Signature

Date

17. **Government Business Partner Intended Use Statement**

Pursuant to 18 U.S.C. section 2721, check the box(es) that correspond to the permissible use(s) that allow the GOVERNMENT BUSINESS PARTNER access to DVS data.

See **Exhibit C for the list of permissible uses**. Check all uses that apply.

☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7

☐ 8 ☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14

Use of Data Requested

☐ **Driver's License Data**

Provide general use and specific examples of how the driver's license data will be used by the GOVERNMENT BUSINESS PARTNER.

_____

_____

☐ **Motor Vehicle Data**

Provide general use and specific examples of how the motor vehicle data will be used by the GOVERNMENT BUSINESS PARTNER.

_____

_____

☐ **Photo Access**

Check the box that applies to the GOVERNMENT BUSINESS PARTNER pursuant to Minnesota Statutes, section 171.07, subdivision 1a.

☐ To criminal justice agencies, as defined in Minnesota Statutes, section 299C.46, subdivision 2, for the investigation and prosecution of crimes, service of process, enforcement of no contact orders, location of missing persons, investigation and preparation of cases for criminal, juvenile, and traffic court, location of individuals required to register under Minnesota Statutes, sections 243.166 or 243.167, and supervision of offenders;

☐ To public defenders, as defined in Minnesota Statutes, section 611.272, for the investigation and preparation of cases for criminal, juvenile, and traffic courts;

☐ To child support enforcement purposes under Minnesota Statutes, section 256.978; and

☐ To a county medical examiner or coroner as required by section Minnesota Statutes, 390.005 as necessary to fulfill the duties under Minnesota Statutes, sections 390.11 and 390.25.

Provide specific examples of how the driver's license photo data will be used by the GOVERNMENT BUSINESS PARTNER pursuant to Minnesota Statutes, section 171.07, subdivision 1a.

_____

☐ Other data access request and authority – Please explain:

_____

I, the undersigned, as an authorized representative of the GOVERNMENT BUSINESS PARTNER, certify by signing this document that the information and statements provided on this document are true and correct, and I agree to the terms and conditions for the intended use of DVS data as defined in **Exhibit A**, **Exhibit B,** and **Exhibit C**, which are attached and incorporated into this agreement by reference.

I understand that pursuant to Minnesota Statutes, section 171.12, subdivision (1a)(b), **the Commissioner must impose disciplinary action of any individual who willfully enters, updates, accesses, shares, or disseminates data in violation of state or federal law. If an individual willfully gained access to data without authorization by law, the Commissioner must forward the matter to the appropriate prosecuting authority for prosecution.**

Government Business Partner	**State**
Signature: _____	Signature: _____
Printed Name: _____	Printed Name: _____
Job Title (no acronyms): _____	Job Title (no acronyms): _____
Date: _____	Date: _____
Email: _____	
Phone Number: _____	

Please email the completed agreement to DVS.DataServices@state.mn.us or fax to (651) 797-1205.

Exhibit A

Minnesota Department of Public Safety
Driver and Vehicle Services Policy

SECURITY AND CONFIDENTIALITY OF DATA AND RECORDS
Policy No. 125-1000

Updated: October 1, 2023

APPLICABILITY

This policy applies to any individual with access to the Department of Public Safety's Driver and Vehicle Services (DVS) information system, including DVS employees and individuals external to DVS, such as deputy registrars, driver license agents, dealers, private entities, and government agencies.

POLICY PURPOSE

The purpose of this policy is to comply with the requirements and responsibilities of Minnesota Statutes, section 171.12, subdivision 1a, to ensure only individuals authorized by law enter, update, or access not public data collected, created, or maintained by the DVS information system.

POLICY STATEMENT

DVS employees and all individuals granted access to the DVS information system ("authorized users") are required to safeguard the not public data in the DVS information system from improper use or disclosure. Not public data is defined by Minnesota Statutes, section 13.02, subdivision 8a as "any government data classified by statute, federal law, or temporary classification as confidential, private, nonpublic, or protected nonpublic."

Access to the DVS information system is granted and authorized only for the purpose of carrying out lawful, assigned work duties during work hours. An authorized user's ability to enter, update, or access data in the system must correspond to the official duties or training level and to the statutory authorization granting access.

All data or information that is created, entered, stored, or processed on or in the DVS information system is the property of DVS. Viewing, distributing, or using DVS data or information for mere curiosity, any personal use, or other non-business purpose is strictly prohibited.

As required by Minnesota Statutes, section 171.12, subdivision 1a, the Commissioner must impose disciplinary action to any individual who willfully enters, updates, accesses, discloses or otherwise makes available data in the DVS information system in violation of federal and state law. An appeal of the disciplinary action is available within the Department of Public Safety. For DVS employees, failure to

SECURITY AND CONFIDENTIALITY OF DATA AND RECORDS
Policy No. 125-1000

comply with this policy may result in disciplinary action up to and including termination.

DEFINITIONS

For the purposes of this policy, the terms listed have the following meaning:

Administrator or supervisor: Person responsible to train and seek authorized access for users of the DVS information system.

Authorized users: DVS employees, contractors, vendors, consultants, interns, volunteers, and all other users who have been authorized by DVS to access the DVS information system.

Disciplinary action: A formal or informal disciplinary measure, including but not limited to requiring corrective action or suspending or revoking the authorized user's access to the DVS information system.

DVS data: All data collected, created, received, maintained, or disseminated by DVS regardless of its physical form, storage media, or conditions of use.

DVS information system: DVS owned, operated, and managed information system (e.g., MNDRIVE, e-Services for Business, etc.).

Family member: Spouse, parents, stepparents, foster parents, father-in-law, mother-in-law, children, stepchildren, foster children, sons-in-law, daughters-in-law, grandparents, grandchildren, brothers, sisters, brothers-in-law, sisters-in-law, aunts, uncles, nieces, nephews, and first cousins.

Not public data: Any government data classified by statute, federal law, or temporary classification as confidential, private, nonpublic, or protected nonpublic. This includes information that identifies an individual including an individual's photograph, social security number, driver's license/identification number, name, address (but not the five-digit zip code), date of birth, telephone number, medical/disability information, and other data classified as private data under the Minnesota Government Data Practices Act, Minnesota Chapter 13, and the federal Driver's Privacy Protection Act, 18 United States Code sections 2721 et seq.

Transactions: All interactions with customers, stakeholders, and legislators, including in-person, simultaneous audio/visual, telephonic, emails, letters, applications, orders, convictions relating to licenses, identification cards, and motor vehicles.

ROLES AND RESPONSIBILITIES

Administrator and/or Supervisor Responsibilities: An administrator or supervisor is responsible for ensuring current and new staff review Policy 125-1000, sign the DVS Data Access Attestation (located

below), and complete an Authorized User Records Access Agreement needed to obtain access to the DVS information system, *before* the staff member accesses the DVS information system. In addition, administrators or supervisors are responsible for ensuring their staff annually review and attest to this policy. Administrators or supervisors shall maintain the initial and annual policy attestation documentation of authorized users. Administrators and supervisors must cooperate with DVS on any audits concerning the access to the DVS information system. Supervisors and administrators shall contact the DVS Data Practices Unit with questions or concerns about this policy.

Authorized User Responsibilities: Authorized users are responsible for following the policy, for accessing the DVS information system only in accordance with this policy, the Authorized User Records Access Agreement, and applicable law, and for contacting their supervisor or administrator, or the DVS Data Practices Unit, with questions or concerns about how this policy applies. If authorized users are unclear if their access of the DVS information system is lawful and appropriate, it is their responsibility to seek clarification before acting.

DVS Division Responsibilities: DVS is responsible for granting, auditing, and revoking access to the DVS information system. For DVS employees, DVS is also responsible for any disciplinary action resulting from non-compliance with this policy, up to and including termination.

GENERAL STANDARDS AND EXPECTATIONS

Authorized users must comply with all provisions of this policy. Authorized users are required to seek clarification if they have questions about this policy and its application.

1. Review and Sign Attestation

All authorized users must review this policy and sign the Security and Confidentiality of Data and Records Attestation (found at the end of this policy) before accessing the DVS information system. In addition, on an annual basis, all authorized users must again review the policy and re-sign the Security and Confidentiality of Data and Records Attestation. Administrators or supervisors shall maintain the initial and annual policy attestation documentation of authorized users.

2. Usernames and Passwords

Authorized users will not share or otherwise disclose their usernames or passwords with anyone, including administrators, supervisors, or technical support staff. All use of security credentials will be presumed to be only that of the assigned authorized user. In the event an authorized user suspects their password is compromised or known to others, the authorized user will immediately change their password and notify their supervisor or administrator, who will then notify DVS Data Practices Unit.

Authorized users will secure computers, laptops, or other electronic or mobile devices that have access to the DVS information system by logging off or “locking” the device whenever it is left unattended.

SECURITY AND CONFIDENTIALITY OF DATA AND RECORDS
Policy No. 125-1000

Authorized users shall not complete a transaction on another authorized user's unattended device.

3. Access to DVS Information System

Only individuals authorized by law may enter, update, or access not public data collected, created, or maintained by the DVS information system. Authorized users' ability to enter, update, or access data in the DVS information system must correspond to the official duties or training level of the individual and to the statutory authorization granting access for that purpose.

Access to the DVS information system is granted and authorized only for the purposes of carrying out assigned work duties and for lawful purposes during work hours. Access to the DVS information system for personal or non-business purposes is not authorized access and constitutes a violation of federal and state law. Misuse or other inappropriate use of the DVS information system, or the improper or unsecured handling of not public data from the DVS information system, should be immediately reported to DVS Data Practices Unit and/or your administrator or supervisor.

Accidental access is not willful unauthorized access. For example, accessing a record on the DVS information system because of a mistyped license plate number or driver's license number, even if mistyped more than once, will not be considered willful misuse of the DVS information system. This accidental access should be noted at the time in your office's record management system. However, if a user intentionally and consciously (not accidentally) accesses the DVS information system and that access was without authorization and for a lawful purpose, that access will be considered misuse whether or not the user knew their access was unauthorized or against the law.

Authorized users who are not authorized to process enhanced driver's licenses, enhanced identification cards, REAL ID compliant driver's licenses, or REAL ID compliant identification cards will not enter, update, access, share, or disseminate DVS data related to these specific types of transactions.

4. Certification Requirement under Minnesota Statutes, section 171.12, subdivision 7b(d)

Authorized users must not use noncompliant (credential that does not meet the REAL ID Act) driver's license or identification card data for civil immigration enforcement purposes or disclose the data to a state or federal government entity that primarily enforces immigration law or to any employee or agent of any such government entity. If the authorized user violates this certification, they may be liable in a civil action brought under Minnesota Statutes, section 13.08, may be subject to criminal penalties under Minnesota Statutes, section 13.09, and may have subsequent requests for noncompliant driver's license or identification card data be denied by the Commissioner.

5. Data Access and Transactions for Authorized Users (Self), Family Members, or Individuals in Same Household

An authorized user is prohibited from accessing the DVS information system for themselves, family members, or individuals residing in the same household as the authorized user. This prohibition includes

accessing your record for training, reference, or comparison purposes. An authorized user may not process transactions in the DVS information system for themselves, family members, or individuals residing in the same household as the authorized user. This access is considered unauthorized.

Requests for special handling of any transaction or action on any type of license, permit or registration involving an authorized user, family member, or individuals in the same household, must be raised with the authorized user's supervisor or administrator to obtain clarification before acting. Administrators or supervisors should develop a procedure directing how these transactions should be handled (e.g., by a supervisor or another designated authorized user). Administrators or supervisors who need further clarification on this policy's application to these types of transactions should contact DVS Data Practices Unit before any unauthorized access or transaction occurs. If an office has only one authorized user, then that authorized user may submit to DVS Data Practices Unit a *Petition for Variance to DVS Policy 125-1000 on Security and Confidentiality of Data and Records for One-Person Office* and receive written approval in advance of the transaction.

6. Monitored Access to the DVS Information System

All queries and responses, and all actions in which data are entered, updated, accessed, shared, or disseminated, must be recorded in a data audit trail. Data contained in the audit trail are public to the extent the data are not otherwise classified by law.

All access to the DVS information system is monitored electronically and maintained in audit files by DVS. DVS reviews the audit files to ensure compliance with state and federal laws, this policy, and the applicable user agreements.

7. Secure data storage and disposal methods

Authorized users are responsible for secure handling, storage, and disposal of documents containing not public data. Authorized users must ensure DVS documents or electronic files containing not public data are stored or destroyed in a manner that does not reveal not public data to others. Authorized users must dispose of all documents containing not public data in the proper locked disposal containers or by secure shredding, meaning shredding documents in a manner that prevents reconstruction or renders them practicably unreadable.

8. Examples of Violations of this Policy

Examples listed in this policy are provided for purpose of illustration and do not comprise an exhaustive list.

The following are unauthorized actions and in violation of this policy:

- sharing usernames and passwords;
- sharing or disseminating data without an authorized business purpose;

- accessing the DVS information system without an authorized business purpose;
- processing or assisting in the processing of fraudulent or unauthorized transactions, such as:
  - certificate of title;
  - registration;
  - permit;
  - driver's license;
  - identification card; and
  - any other DVS document or license.
- requesting another authorized user to commit any actions prohibited in this policy;
- receiving or attempting to receive a benefit, privilege, exemption, or advantage related to drivers' licensing, motor vehicle registration, or titling due to their title or employment;
- accessing data from an unauthorized computer;
- changing a record without an authorized business purpose;
- tampering with a record; and
- accessing the DVS information system during any DVS issued suspension or revocation.

9. Penalties for violation of this policy

If this policy is violated, the following penalties may be assessed:

- The Commissioner must impose disciplinary action to any individual who willfully enters, updates, accesses, shares, or disseminates data in violation of state or federal law.
- If an individual willfully gained access to DVS data without authorization by law, the Commissioner must forward the matter to the appropriate prosecuting authority for prosecution. Criminal and/or civil liability may be implicated for unauthorized use of the DVS information system and the not public data contained in the system.
- For DVS employees, DVS may impose corrective action, including counseling or job reassignment, or disciplinary action up to and including termination.

AUTHORITIES

- 18 United States Code sections 2721 et seq., Driver's Privacy Protection Act
- Minnesota Statutes, Chapter 13, Minnesota Government Data Practices Act
- Minnesota Statutes, section 171.07, subdivision 1a, Driver and vehicle services information system; security and auditing
- Minnesota Statutes, section 171.12, subdivision 7b(d), Data privacy; noncompliant license or identification card
- Minnesota Rule 1205.0200, subpart 9, Private data

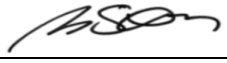
SECURITY AND CONFIDENTIALITY OF DATA AND RECORDS
Policy No. 125-1000

- Department of Public Safety Policy 5100, Acceptable Use of Department Computers, Electronic Equipment, Information Systems and Resources

ADDITIONAL RESOURCES

- DVS Data Practices Unit at DVS.DataServices@state.mn.us
- Your Individual Records Access Agreement for access to the DVS information system
- Frequently Asked Questions - Accessing Driver and Vehicle Services Data and Records
- Petition for Variance to DVS Policy 125-1000 on Security and Confidentiality of Data and Records for One-Person Office
- For DVS employees - Minnesota Statutes, section 43A.38, Code of Ethics for Employees in the Executive Branch

REVISION HISTORY
Policy Owner: Driver and Vehicle Services, Data Practices (DVS.DataServices@state.mn.us)
Effective Date: 10/01/2023

Approved By: 
Name/Title: Pong S. Xiong, Director, Driver, and Vehicle Services
Date: 09/12/2023

Revision	Date	Author	Summary of Changes
0.0	11/23/2015	DVS	
1.1	12/20/2017	DVS Data Practices	Incorporating Minn. Stat. § 171.12
1.2	01/31/2022	DVS Data Practices	Added links to additional resources, forms, and other updates
1.3	10/01/2023	DVS Data Practices	Added information about Minn. Stat. § 171.12, subd. 7b(d), Minn. Stat. § 171.12 1a, and other clarifying language
1.4			
1.5			
1.6			

SECURITY AND CONFIDENTIALITY OF DATA AND RECORDS
Policy No. 125-1000

MINNESOTA DEPARTMENT OF PUBLIC SAFETY
DRIVER AND VEHICLE SERVICES DIVISION

Security and Confidentiality of Data and Records Access Attestation

Check One: ☐ NEW ☐ ANNUAL REATTESTATION

Administrator/Supervisors

1) Give authorized user a copy of DVS Policy 125-1000, Security and Confidentiality of Data and Records.
2) If DVS employee, submit signed attestation to your supervisor.
3) If non-DVS employee, the administrator or supervisor retains a copy of the signed attestation statement in case of audit.

Authorized User

I have read and understand this policy and had the opportunity to ask questions and discuss them with my supervisor or administrator.

I understand that, as required by Minnesota Statutes, section 171.12, subdivision 1a(b), the Commissioner will impose disciplinary action if I willfully enter, update, access, share, or disseminate data in violation of state or federal law. This includes accessing my driver or vehicle records and those of my family or any individual residing in my household that are maintained in the DVS information system.

By signing this attestation, I attest that I am not currently the subject of any DVS issued suspension or revocation.

For DVS employees, I understand that failure to comply with this policy may result in disciplinary action up to and including termination.

I also understand if I willfully gain access to DVS data without authorization by law, the Commissioner must forward the matter to the appropriate prosecuting authority for prosecution.

_____
(Print Name)

_____ _____
(Signature) (Date)

Exhibit B

Access to Driver License and Motor Vehicle records is governed by Minnesota Statutes, sections 168.346, 171.12, and 18 U.S.C. sections 2722-2725.

Under 18 U.S.C. section 2722, the following are unlawful acts:

(a) PROCUREMENT FOR UNLAWFUL PURPOSE. — It shall be unlawful for any person knowingly to obtain or disclose personal information, from a motor vehicle record, for any use not permitted under section 2721(b) of this title.

(b) FALSE REPRESENTATION. — It shall be unlawful for any person to make false representation to obtain any personal information from an individual's motor vehicle record.

Under 18 U.S.C. section 2723, the following penalty may apply to unlawful acts:

(a) CRIMINAL FINE. — A person who knowingly violates this chapter shall be fined under this title.

18 U.S.C. section 2724, provides for the following Civil action:

(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 attorneys' fees and other litigation costs reasonably incurred; and

(4) such other preliminary and equitable relief as the court determines to be appropriate.

Under 18 U.S.C. section 2725, motor vehicle record is defined as:

(1) "motor vehicle record" means any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles.

Exhibit C

Permissible Uses of Motor Vehicle Data

as provided in United States Code, Title 18, Section 2721

(1) For use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a Federal, State, or local agency in carrying out its functions.

(2) For use in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; performance monitoring of motor vehicles, motor vehicle parts and dealers; motor vehicle market research activities, including survey research; and removal of non-owner records from the original owner records of motor vehicle manufacturers.

(3) For use in the normal course of business by a legitimate business or its agents, employees, or contractors, but only—

  (A) to verify the accuracy of personal information submitted by the individual to the business or its agents, employees, or contractors; and

  (B) if such 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, the individual.

(4) 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 the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a Federal, State, or local court.

(5) For use in research activities, and for use in producing statistical reports, so long as the personal information is not published, redisclosed, or used to contact individuals.

(6) For use by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with claims investigation activities, antifraud activities, rating or underwriting.

(7) For use in providing notice to the owners of towed or impounded vehicles.

(8) For use by any licensed private investigative agency or licensed security service for any purpose permitted under this subsection.

(9) For use by an employer or its agent or insurer to obtain or verify information relating to a holder of a commercial driver's license that is required under chapter 313 of title 49.

(10) For use in connection with the operation of private toll transportation facilities.

(11) For any other use in response to requests for individual motor vehicle records if the State has obtained the express consent of the person to whom such personal information pertains.

(12) For bulk distribution for surveys, marketing or solicitations if the State has obtained the express consent of the person to whom such personal information pertains.

(13) For use by any requester, if the requester demonstrates it has obtained the written consent of the individual to whom the information pertains.

(14) 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.