



MINNESOTA DEPARTMENT OF PUBLIC SAFETY  
 DRIVER AND VEHICLE SERVICES  
**RECORDS ACCESS AGREEMENT**  
 DEALERSHIPS

**FEIN** \_\_\_\_\_

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

an owner or an officer of \_\_\_\_\_

a licensed Minnesota dealership (hereinafter "DEALERSHIP"), assigned dealer number \_\_\_\_\_

If you are a towing company; please provide the following:

Towing License # \_\_\_\_\_ Licensing Authority \_\_\_\_\_

**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") record information system for a DEALERSHIP.**

1. Access to the DVS record information system is restricted to DEALERSHIP personnel who need access to perform their job duties.
2. The DVS data obtained by the DEALERSHIP will only be used in the normal course of DEALERSHIP business to verify the accuracy of personal information submitted by an individual for the purchase or sale of a motor vehicle, or to prevent fraud (18 U.S.C. § 2721(b)(3a)(3b)). Access is permitted to place a held for resale or other type of title notification flag to the record (18 U.S.C. § 2721(b)(1)).
3. The DEALERSHIP will not use DVS data for personal or non-business purposes. Any such use is in violation of state and federal laws.
4. The DEALERSHIP is responsible for training all 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(s) is retained by the DEALERSHIP and submitted to the STATE upon request. (See **Exhibit A**.)
5. The DEALERSHIP will require each individual who has a business need to access the DVS data to sign an *Individual Access Agreement* regarding usage and dissemination of DVS data. This individual agreement is maintained by the DEALERSHIP and submitted to the STATE upon request.
6. The DEALERSHIP will disable a user's access within three (3) days of an assignment change or when no longer employed.
7. The DEALERSHIP understands each user is assigned a unique username, and the user's password information will not be shared with anyone, including other employees or their supervisors.
8. The DEALERSHIP understands that improper use or dissemination of DVS data will result in **permanent loss of record access** as well as criminal and civil penalties under both state and federal laws.

## 9. Information Security

The DEALERSHIP is required to secure and protect the DVS data requested in this agreement. Respond to the questions below to indicate how information security will be maintained:

- a. How will electronic/paper copies of records be securely stored?
  
  
  
  
  
  
  
  
  
  
- b. What type of security software do you use for your online computer terminals?
  
  
  
  
  
  
  
  
  
  
- c. DEALERSHIP users must maintain a way to verify work-related searches (see section 13 below). This record system must be maintained for at least five (5) years from the date of the search and must be presented to the state upon request. How will your business meet the requirements to maintain a record system for work related searches?
  
  
  
  
  
  
  
  
  
  
- d. What is the authentication method used to access your computer?

## 10. Reports of Misuse

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

## 11. Liability

The DEALERSHIP 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 DEALERSHIP or the DEALERSHIP's users. This clause will not be construed to bar any legal remedies the DEALERSHIP may have for the STATE's failure to fulfill its obligations under this agreement.

## 12. Government Data Practices

The DEALERSHIP and the STATE must comply with the Minnesota Government Data Practices Act, Minn. Stat. § 13 and 18 U.S.C. § 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 DEALERSHIP under this agreement. The civil remedies of Minn. Stat. §§ 13.08 and 13.09 and 18 U.S.C. § 2721 apply to the dissemination of the data referred to in this clause by either the DEALERSHIP or the STATE. (See **Exhibit B** and **Exhibit C**.)

## 13. Audits

The STATE maintains an electronic log of data accessed through the DVS record information system. This electronic log includes, in part, the user name, date, time, IP address and the data searched.

The DEALERSHIP 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 DEALERSHIP'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 DEALERSHIP understands that failure to respond to an audit report request with findings may result in suspension or cancellation of the DEALERSHIP's access.

Audits will be conducted at the DEALERSHIP's expense.

## 14. Termination

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

15. **Delegation of Data Administrator**

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

**Administrator Responsibilities**

- Provide the new user with training on the proper use and dissemination of DVS data
- Obtain a signed individual agreement
- Provide the user with the means for access
- Verify the identity of the user via a current state issued ID or driver license (DL)
- Assign appropriate access to users
- Remove access when a user no longer needs access due to an assignment change or is no longer employed

*Please attach a legible copy of your current state issued DL or ID card to verify your identity. Without a copy of your DL or ID card, DVS is unable to provide you with access to record information system.*

\_\_\_\_\_  
Administrator Legal Name (please print or type)

\_\_\_\_\_  
User Specific Email Address

\_\_\_\_\_  
Phone Number

Administrator Attestation:

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

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

I, the undersigned, as an authorized representative of the DEALERSHIP, 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 B** and **Exhibit C**, which are attached and incorporated into this agreement by reference.

I understand that pursuant to Minn. Stat. § 171.12(1a)(b), **the Commissioner will immediately and permanently revoke access of any staff who willfully enters, updates, accesses, shares, or disseminates data in violation of state or federal law. The Commissioner will forward any violation of state or federal law to the appropriate authority for prosecution.**

**Dealership Owner/Officer**

**State**

Signature: _____	Signature: _____
Printed Name: _____	Printed Name: _____
Title (no acronyms): _____	Title (no acronyms): _____
Date: _____	Date: _____
Email: _____	
Phone Number: _____	

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

## Exhibit A

# SECURITY AND CONFIDENTIALITY OF DATA & RECORDS Driver and Vehicle Services

Policy Number: 125-1000

### **POLICY:**

Access to Driver and Vehicle Services (DVS) data is granted and authorized only during work hours and for the purposes of carrying out assigned job duties.

Effective October 1, 2018, the Commissioner will immediately and permanently revoke authorization of any individual who willfully enters, updates, accesses, shares, or disseminates data in violation of state law. [Minn. Stat. § 171.12\(1a\)\(b\)](#).

The Commissioner will forward any violations of state or federal law to the appropriate authority for prosecution. [Minn. Stat. § 171.12\(1a\)\(b\)](#).

### **AUTHORITY:**

18 U.S.C. §§ 2721 et seq., Driver's Privacy Protection Act

[Minn. Stat. § 13](#), Minnesota Government Data Practices Act

[Minn. Stat. § 168.345\(1\)](#), Information by telephone

[Minn. Stat. § 171.07\(1\)\(a\)](#), Filing photograph or image; data classification

[Minn. Stat. § 171.12\(1a\)\(b\)](#), Driver and Vehicle Services information system; security and auditing

[Minn. R. 1205.0200, subp. 9](#), Private data

[DPS Policy 5100](#), Acceptable Use of Department Computers, Electronic Equipment, Information Systems and Resources

### **APPLICABILITY:**

All DVS employees and individuals who have access to DVS data.

### **PURPOSE:**

To ensure all DVS employees and individuals who have access to DVS data are informed of Minnesota statutes and federal laws regarding the appropriate access and use of division records.

### **DEFINITIONS:**

Personal Information - identifying data including, but not limited to, an individual's photograph, social security number, driver's license number, name, address (not zip code), date of birth, telephone number, and medical/disability information.

Staff - for the purposes of this policy, staff means DVS employees and any individuals who have access to DVS data.

Transactions - all interactions with customers, stakeholders, and legislators, including but not limited to, phone inquiries, emails, letters, applications, orders, convictions relating to licenses, identification cards, and motor vehicles. 18 U.S.C. §§ 2721 et seq.

### **PROCEDURES:**

- A. All staff must read this policy and sign the "DVS Data Access Attestation Statement," 125-1000a (attached) on the first day of employment.
- B. Each January, all staff must review this policy and sign the "DVS Data Access Attestation Statement," 125-1000a (attached).
- C. *Usernames and Passwords*
  1. Staff will not share usernames and passwords with anyone, including supervisors and technical support staff.
  2. In the event that staff suspect their password is compromised or known to others, staff will change their password and notify their supervisor immediately.

## **Exhibit A - Continued**

### **D. Access to DVS data**

1. Staff will only access DVS data during work hours.
2. Staff will only access DVS data for the purposes of carrying out assigned job duties and for lawful purposes.
3. Staff will not enter, update, access, share, or disseminate DVS data to anyone unless authorized by state and federal law.
4. Staff 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.

### **E. Transactions and records relating to individuals known to staff**

1. Staff will not process any transactions for themselves or for friends, family, or other employees.
2. Staff will not check their own records or the records of friends, family, or other employees.
3. All requests for special handling of any transaction or action on any type of license, permit or registration involving staff or friends, family, or other employees must be turned over to a supervisor.

### **F. Telephone release of data**

1. Staff will not release non-public vehicle registration information over the telephone, except to the following, ONLY after verifying the requestor is from one of the following:
  - a. law enforcement agencies
  - b. personnel of other states that register vehicles
  - c. authorized agents of the Department of Public Safety (DPS)

### **G. Monitored access to DVS data**

1. All record access through all verification systems is monitored electronically and maintained in audit files by the Data Practices Unit.
2. The audit files are reviewed periodically to ensure staff compliance with DVS policy and applicable state and federal laws.

### **H. Secure data storage and disposal methods**

1. Staff are responsible for secure handling, storage and disposal of documents containing personal information that identifies an individual.
2. Staff must ensure DVS documents or electronic files that contain personal information are stored or destroyed in a manner that does not reveal personal information to others.
3. Staff must dispose of all documents that contain personal information in the proper locked disposal containers.

### **I. The following unauthorized actions are violations of this policy:**

1. changing or tampering with records
2. sharing or disseminating data
3. accessing records with no business purpose
4. processing or assisting in processing of fraudulent or unauthorized:
  - a. certificate of title
  - b. registration
  - c. permit
  - d. driver's license
  - e. identification card
  - f. any other DVS document or license

## **Exhibit A - Continued**

### *I. continued*

5. requesting another staff commit any actions prohibited in this policy
6. receiving or attempting to receive an advantage for driver's licensing or motor vehicle registration or titling due to their title or employment
7. accessing data from an unauthorized computer
8. sharing user names and passwords

### *J. Penalties for violation of this policy*

1. The Commissioner will immediately and permanently revoke the authorization of any individual who willfully enters, updates, accesses, shares, or disseminates data in violation of state law. Minn. Stat. § 171.12(1a)(b).
2. The Commissioner will forward any violations of state or federal law to the appropriate authority for prosecution. Minn. Stat. § 171.12(1a)(b).
3. Corrective action, including counseling and/or job reassignment
4. Disciplinary action, including discharge
5. Possible criminal prosecution, fines, and civil action

### **REVIEW:**

Annually

### **REFERENCES:**

[Minn. Stat. § 43A.38](#), Code of Ethics for Employees in the Executive Branch

### **ATTACHMENTS:**

"DVS Data Access Attestation Statement," 125-1000a

### **SUPERSESION:**

DVS Policy, "Security and Confidentiality of Data & Records" November 23, 2015

**MINNESOTA DEPARTMENT OF PUBLIC SAFETY DRIVER & VEHICLE SERVICES DIVISION**

**Security & Confidentiality of Data & Records DVS Data Access Attestation Statement**

Policy Number: 125-1000

**Check One:**  New Employee       Annual

**Supervisors**

- 1) Give staff a copy of DVS policy 125-1000, Security and Confidentiality of Data and Records.
- 2) If DVS staff, submit this attestation statement to the DVS Training & Development Unit.
- 3) If non-DVS staff, the supervisor retains a copy of the signed attestation statement in case of audit.

**Employee**

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

I understand that pursuant to Minn. Stat. § 171.12(1a)(b), the Commissioner will immediately and permanently revoke the authorization of any individual who willfully enters, updates, accesses, shares, or disseminates data in violation of state or federal law.

The Commissioner will forward any violation of state or federal law to the appropriate authority for prosecution.

Print Name: \_\_\_\_\_

Signature \_\_\_\_\_ Date: \_\_\_\_\_

## **Exhibit B**

Access to Driver License and Motor Vehicle records is governed by Minn. Stat. §§ 168.346, 171.12, 171.12(7a) and 18 U.S.C. §§ 2722-2725.

### **Under 18 U.S.C. § 2722 the following are unlawful acts:**

- (a) Procurement for Unlawful Purposes. -- 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. § 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. § 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. § 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 18 U.S.C. § 2721

- 1) For use by any government agency, including 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 agencies, employees, or contractors; and (B) if such information as so submitted is not correct or is no longer correct, to obtain 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, re-disclosed, or used to contact individuals.
- 6) For use by any insurer or insurance support organization, or by 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 the Commercial Motor Vehicle Safety Act of 1986 (49 U.S.C. App. 3131 *et seq.*).
- 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 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. **List specific statutory authorization.**