



State of Minnesota

Income Contract

SWIFT Contract Number: 261780

This Contract is between the State of Minnesota, acting through its Commissioner of Public Safety on behalf of the Driver and Vehicle Services division ("DVS" or "State"), and Safety Holdings, Inc. and its subsidiaries and affiliates, whose designated business address is 5445 DTC Parkway Ste., 950 Greenwood Village, Colorado 80111 ("Purchaser"). The State and Purchaser may be referred to jointly as "Parties."

Recitals

1. Under Minnesota Statutes § 168.327, subdivision 4, the State is empowered to enter into income contracts.
2. The Purchaser uses Minnesota driving records ("DVS Data") for a variety of products and services specified in the Driver's Privacy Protection Act ("DPPA") under Title 18 U.S.C. § 2721, and the Minnesota Government Data Practices Act ("MGDPA"), Minnesota Statutes Chapter 13, including, but not limited to, insurance industry support and employer support.
3. The State represents that it is duly qualified and agrees to provide the services described in this contract.

Contract

1. Term of Contract

- 1.1 Effective Date.** December 23, 2024, or the date the State obtains all required signatures under Minnesota Statutes section 16C.05, subdivision 2, whichever is later.
- 1.2 Expiration Date.** December 22, 2029, or until all obligations have been satisfactorily fulfilled, whichever occurs first.

2. State's Duties

State will:

- 2.1** Create a daily file containing DVS Data.
- 2.2** Prepare the DVS Data for secure transmittal to Purchaser.
- 2.3** Assure the DVS Data is encrypted prior to transmittal.
- 2.4** Transmit the DVS Data to Purchaser.

3. Purchaser's Duties

Purchaser will:

- 3.1** Refrain from using any information identified in or derived from DVS Data obtained from the State for personal or non-business purposes. Such use may result in the violation of federal or state laws, rules and regulations, and policies.
- 3.2** Restrict access to DVS Data exclusively and solely to personnel who need access to perform their job duties.
- 3.3** Develop and maintain a method of identifying each entity or person that receives DVS Data containing personal information as defined in **Exhibit A**, which is attached and incorporated into

this Contract. Record the date DVS Data was transmitted to the entity or person, and the permissible use or explanation why or how the DVS Data will be used. The records must be maintained and made available to the State for inspection upon request. *See* Section 10 below regarding audit procedures.

- 3.4** Educate all personnel on the proper use and dissemination of DVS Data using Exhibit A as the fundamental basis for such education. Training materials and certification must be maintained and made available to the State for inspection upon request. *See* Section 10 below regarding audit procedures.
- 3.5** Comply with the State's mandate for disciplinary action for any individual who willfully enters, updates, accesses, shares, or disseminates DVS Data in violation of state or federal law.
- 3.6** Establish a DPPA compliance program and designate a compliance director to oversee the program.
- 3.7** Insert language into each customer contract requiring that the customer: 1) maintain the confidentiality of DPPA-regulated information; 2) identify how the information is to be used; 3) use the information only for permissible purposes under state and federal law; and 4) allow Purchaser to terminate a customer's access at any time.
- 3.8** Successfully and timely complete a data and system security assessment provided by the State and address any deficiencies, prior to receiving any DVS Data. Failure to do so will result in immediate termination of this contract by the State. The State may request an updated security assessment at any time during the term of this contract. Purchaser agrees to immediately address and remediate any concerns or issues identified by DVS.
- 3.9** Protect DVS Data by:
 - 3.9.1** Refraining from use of DVS Data in a manner that contravenes the public policy of the State or the general well-being of its customers. Purchaser's authorization to use DVS Data is limited to the purposes stated in Chapter 13 and in compliance with the DPPA;
 - 3.9.2** Refraining from use of personal names or addresses identified in or derived from DVS Data for the purpose of selling or offering for sale any property or service to any person identified or to any person residing at the address identified;
 - 3.9.3** Refraining from the sale or distribution of personal names or addresses identified in or derived from DVS Data for the purpose of allowing the person identified to sell or offer for sale any property or service to any person identified or to any person residing at the address identified;
 - 3.9.4** Refraining from use of any information identified in or derived from DVS Data in violation of the terms of this Contract including the distribution of encrypted DVS Data outside the purview of this Contract;
 - 3.9.5** Notifying the State as soon as practicable but no longer than twenty-four (24) hours after discovering any breach or misuse of DVS Data, such notification being provided via email to the State's Authorized Representative identified in Clause 5. Notification shall include a list of all records, information, and data that the Purchaser believes or has reason to believe to have been lost, compromised, or misused. The requirement to report a breach or misuse survives the expiration or termination of this Contract;
 - 3.9.6** Notifying the State as soon as practicable but no longer than 24 hours after any computer security problem, investigation, misplaced data, or other negative corporate or client event that has compromised personal information in DVS Data, such notification being provided via email to the State's Authorized Representative identified in Clause 5;
 - 3.9.7** Refraining from disseminating or publishing any personal information acquired in DVS Data on the Internet, nor allowing any other person to disseminate or publish any personal information

acquired in DVS Data on the Internet;

3.9.8 Complying with all terms and conditions of the State's Policy 125-1000, attached as **Exhibit A**; and

3.9.9 Agreeing that personal information contained in DVS Data shall not be stored outside the United States by the Purchaser either electronically or otherwise.

3.9.10 When this Contract expires or is terminated, all DVS Data must be deleted, and the Purchaser shall provide certification to the State that all DVS Data has been deleted.

4. Payment

Purchaser will pay for performance by the State under this Contract as follows:

4.1 The monthly cost of the subscription service is governed by Minnesota Statutes § 168.327, subdivision 4(b), which is subject to change; and,

4.2 The cost per record is governed by Minnesota Statutes § 168.327, subdivision 4(c), which is subject to change.

The State will invoice Purchaser, and Purchaser will remit payment to the State within thirty (30) calendar days of receiving the invoice, such remittance to be mailed to:

Minnesota Department of Public Safety
Driver and Vehicles Services Division
Attn: Cashiers
445 Minnesota Street, Suite 162
Saint Paul, MN 55101-5162

5. Authorized Representatives

The State's Authorized Representative is the following individual, or his successor:

Name: Pong Xiong, Director of Driver and Vehicle Services
Address: 445 Minnesota Street
Saint Paul, MN 55104
Telephone: 651-201-7580
Email Address: pong.xiong@state.mn.us

The Purchaser's Authorized Representative is the following individual, or his successor. If the Purchaser's Authorized Representative changes at any time during this Contract, the Purchaser must notify the State via email within ten (10) calendar days:

Name: John Diana
Address: 5445 DTC Parkway Ste 950
Greenwood Village, CO 80111
Telephone: 720-213-5469
Email Address: jdiana@sambasafety.com

6. Assignment, Amendments, Waiver, and Contract Complete

- 6.1 Assignment.** The Purchaser may neither assign nor transfer any rights or obligations under this Contract without the prior written consent of the State and a fully executed assignment agreement, executed and approved by the same parties who executed and approved this Contract, or their successors in office.
- 6.2 Amendments.** Any amendment to this Contract must be in writing and will not be effective until it has been executed and approved by the same parties who executed and approved the original contract, or their successors in office.
- 6.3 Waiver.** If the State fails to enforce any provision of this Contract, that failure does not waive the provision or its right to enforce it.
- 6.4 Contract Complete.** This Contract contains all negotiations and agreements between the State and the Purchaser. No other understanding regarding this Contract, whether written or oral, may be used to bind either party.

7. Indemnification

- 7.1** In the performance of this Contract, the Indemnifying Party must indemnify, save, and hold harmless the State, its agents, and employees, from any claims or causes of action, including attorney's fees incurred by the State, to the extent caused by Indemnifying Party's:
1. Intentional, willful, or negligent acts or omissions; or
 2. Actions that give rise to strict liability; or
 3. Breach of contract or warranty.

The Indemnifying Party is defined to include the Purchaser and any third party that has a business relationship with the Purchaser or Purchaser's agents or employees, and to the fullest extent permitted by law. The indemnification obligations of this section do not apply in the event the claim or cause of action is the result of the State's sole negligence. This clause will not be construed to bar any legal remedies the Indemnifying Party may have for the State's failure to fulfill its obligation under this Contract.

- 7.2** Nothing within this Contract, whether express or implied, shall be deemed to create an obligation on the part of the State to indemnify, defend, hold harmless or release the Indemnifying Party. This shall extend to all agreements related to the subject matter of this Contract, and to all terms subsequently added, without regard to order of precedence.

8. Government Data Practices

The Purchaser and State must comply with the Minnesota Government Data Practices Act, Minnesota Statutes Chapter 13, and Title 18 U.S.C. § 2721, as they apply to all data provided by the State under this Contract and as it applies to all data created, collected, received, stored, used, maintained, or disseminated by Purchaser under this Contract. The civil remedies of Minnesota Statutes §§ 13.08 and 13.09 and Title 18 U.S.C. §§ 2721-2725 apply to the dissemination of the data referred to in this clause by either Purchaser or the State as outlined in **Exhibit B** and **Exhibit C**, which are attached and incorporated into this Contract.

If the Purchaser receives a request to release the data referred to in this clause, the Purchaser must immediately notify and consult with the State's Authorized Representative as to how the Purchaser should respond to the request. The Purchaser's response to the request shall comply with applicable law.

The Purchaser must ensure that customers accessing DVS data will not use noncompliant (i.e., credential that does not meet the REAL ID Act requirements) driver's license or identification card data for civil immigration enforcement purposes or disclose the data to any federal government entity that primarily enforces

immigration law or to any employee or agency of any such government entity in accordance with Minnesota Statutes § 171.12, subdivision 11. See **Exhibit D**.

9. Publicity and Endorsement

9.1 Publicity. Any publicity regarding the subject matter of this Contract must identify the State as the sponsoring agency and must not be released without prior written approval from the State's Authorized Representative. For purposes of this provision, publicity includes notices, informational pamphlets, press releases, information posted on corporate or other websites, research, reports, signs, and similar public notices prepared by or for the Purchaser individually or jointly with others, or any subcontractors, with respect to the program, publications, or services provided resulting from this Contract.

9.2 Endorsement. The Purchaser must not claim that the State endorses its products or services.

10. Audit Information

10.1. Under Minnesota Statutes § 16C.05, subdivision 5, the Purchaser's books, records, documents, training materials, and accounting procedures relevant to this Contract are subject to examination by the State and/or the State Auditor or Legislative Auditor, as appropriate, for a minimum of six (6) years from the expiration or termination of this Contract.

10.2. The Purchaser must maintain the ability to provide the State with a particular record and date of the request by an entity for a minimum of five (5) years from the date of inquiry.

10.3. Under Minnesota Statutes § 168.327, subdivision 6, the Purchaser must annually engage an independent third party to audit its uses of bulk data and its information technology security procedures, including: (1) the methods and practices employed in the processing methods and use of driver and vehicle services data; (2) compliance with the certification required under Minnesota Statutes § 171.12, subdivision 7b, paragraph (d), and address any material deficiencies.

10.4. Each February, the Purchaser must provide the State with an updated list of each person or entity that received DVS Data from the Purchaser and the permissible use of each person or entity. The State may request an updated client list at any time during the Contract period.

11. Governing Law, Jurisdiction, and Venue

Minnesota law, without regard to its choice-of-law provisions, governs this contract. Venue for all legal proceedings out of this contract, or its breach, must be in the appropriate state or federal court with competent jurisdiction in Ramsey County, Minnesota.

12. Data Disclosure

Under Minn. Stat. § 270C.65, subd. 3, and other applicable law, the Purchaser consents to disclosure of its social security number, federal employer tax identification number, and Minnesota tax identification number to federal and state agencies, and state personnel involved in the payment of state obligations. These identification numbers may be used in the enforcement of federal and state laws which could result in action requiring the Purchaser to file state tax returns, pay delinquent state tax liabilities, if any, or pay other state liabilities.

13. Termination

The State or Purchaser may terminate this Contract at any time, with or without cause, upon thirty (30) days written notice to the other party.

14. Use of DVS Data

Pursuant to Title 18 U.S.C. § 2721, Purchaser will check the box(es) below that correspond to the permissible use(s) for which Purchaser requests access to DVS Data.

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

☒	☐	☒	☒	☐	☒	☐	☐	☒	☐	☐	☐	☒	☐
1	2	3	4	5	6	7	8	9	10	11	12	13	14

Provide a description of the use of the DVS Data:

FILL IN INFORMATION

In compliance with the Driver's Privacy Protection Act exemptions below, Safety Holdings, Inc. is a conduit of information to insurance customers to assist them in underwriting and, where permitted, claims invitation. Information also is provided to employment customers for risk management purposes. Certain customers, such as commercial driving schools, obtain information, where permitted, for legitimate business uses.

15. Survival of Terms

The following clauses survive the expiration or cancellation of this Contract: Indemnification; Government Data Practices; Publicity and Endorsement; Audit Information; Governing Law, Jurisdiction, and Venue; and Data Disclosure.

1. Purchaser: Safety Holdings, Inc.

The Purchaser certifies that the appropriate person(s) has(have) executed this Contract on behalf of the Purchaser as required by applicable articles, bylaws, resolutions, or ordinances.

Print Name: DocuSigned by: John Diana
 Signature: John Diana
 Title: General Counsel Date: 12/20/2024

2. State: Department of Public Safety; Driver and Vehicle Services Division

With delegated authority

Print Name: DocuSigned by: Pong Xiong
 Signature: Pong Xiong
 Title: Director - Driver and Vehicle Services Date: 12/24/2024

3. Commissioner of Administration

As delegated to The Office of State Procurement

Print Name: DocuSigned by: Sherry Van Horn
 Signature: Sherry Van Horn
 Title: Contracts Specialist Date: 12/26/2024
 Admin ID: 94779

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

Exhibit A



Minnesota Department of Public Safety Driver and Vehicle Services Policy

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

Exhibit A



Minnesota Department of Public Safety Driver and Vehicle Services Policy

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. 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

Exhibit A



Minnesota Department of Public Safety Driver and Vehicle Services Policy

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

Exhibit A



Minnesota Department of Public Safety Driver and Vehicle Services Policy

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;

Exhibit A



Minnesota Department of Public Safety Driver and Vehicle Services Policy

- 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
- 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

Exhibit A



Minnesota Department of Public Safety Driver and Vehicle Services Policy

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			

Exhibit A



Minnesota Department of Public Safety Driver and Vehicle Services Policy

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)

Exhibit B

Access to Driver License and Motor Vehicle records is governed by Minnesota Statutes sections 168.346 and 171.12 subdivisions 7 and 7a, and United States Code, Title 18, Sections 2722 through 2725.

Under United States Code, Title 18, Section 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 United States Code, Title 18, 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.

United States Code, Title 18, 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 United States Code Title 18, Section 2725 motor vehicle record is defined as:

- (a) "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 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. 2710 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.**

Exhibit D

Certification of Use and Disclosure of Certain Data

CERTIFICATION:

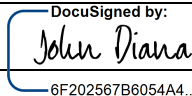
The Purchaser and customers of the Purchaser who access DVS Data must not use noncompliant (i.e., a credential that does not meet the REAL ID Act) driver's license or identification card data for civil immigration enforcement purposes or disclose any of the data to any federal government entity that primarily enforces immigration law or to any employee or agent of any such government entity. Such entities include but are not limited to: U.S. Immigration and Customs Enforcement (ICE), U.S. Customs and Border Patrol (CBP), U.S. Citizenship and Immigration Services (USCIS), and U.S. Homeland Security (DHS).

Pursuant to Minn. Stat. § 171.12, subd. 7b, if the data purchaser violates this certification, the data purchaser may be liable in a civil action brought under Minn. Stat. § [13.08](#), may be subject to criminal penalties under Minn. Stat. § [13.09](#), may have subsequent requests for noncompliant driver's license or identification card data be denied by the commissioner, and may permanently lose access to DVS Data.

By signing this certification, the data purchaser agrees to the terms of the certification and will be held responsible for the compliance of any user of the data.

Name: John Diana

Title: General Counsel

Signature:  6F202567B6054A4...

Date: 12/20/2024