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, subd. (1a)(b).

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

AUTHORITY:
18 U.S.C. §§ 2721 et seq., Driver's Privacy Protection Act
Minn. Stat. Ch. 13, Minnesota Government Data Practices Act
Minn. Stat. § 168.345, subd. 1, Information by telephone
Minn. Stat. § 171.07, subd. 1a, Filing photograph or image; data classification
Minn. Stat. § 171.12, subd. (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.

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

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, subd. (1a)(b).

2. The Commissioner will forward any violations of state or federal law to the appropriate authority for prosecution. Minn. Stat. § 171.12, subd. (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

SUPERSESSION:
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

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, Subd. 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)