



State of Minnesota

Income Contract

SWIFT Contract Number: **207570**

This Contract is between the State of Minnesota, acting through its Commissioner of Public Safety on behalf of the Driver and Vehicle Services division ("State"), and Passport Labs, Inc., whose designated business address is 128 South Tryon Street, Suite 1000, Charlotte, North Carolina, 28202, ("Purchaser"). The State and Purchaser may be referred to jointly as "Parties."

Recitals

1. Under Minnesota Statutes section 168.327, subdivision 5b, the State is empowered to enter into income contracts.
2. The Purchaser uses Minnesota motor vehicle records ["DVS Data"] to send parking ticket delinquency notices and toll road invoices to the registered vehicle owners in accordance with the Driver's Privacy Protection Act ["DPPA"] and Minnesota state statutes.
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 1, 2021, or the date the State obtains all required signatures under Minnesota Statutes section 16C.05, subdivision 2, whichever is later.
- 1.2 Expiration Date.** November 30, 2026, or until all obligations have been satisfactorily fulfilled, whichever occurs first.

2. State's Duties

State will:

- 2.1** Create a weekly file containing the DVS Data that corresponds with the date and license plate that the Purchaser provides.
- 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 resulting in 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, 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.
- 3.4** Educate all personnel on the proper use and dissemination of DVS Data using Exhibit A as the fundamental basis for such education.
- 3.5** Comply with the Commissioner of Public Safety's mandate for immediate and permanent revocation of the authorization of 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 Purchaser's customer contracts requiring customers who obtain personal information to:
 - 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; and 4) allow Purchaser to terminate a customer's access if necessary.
- 3.8** Provide the State a document ["Plan"] outlining the steps or methods taken to secure and protect DVS Data, such document to be submitted to the State within thirty (30) calendar days of execution of this Contract. The Plan must address the following issues:
 - 3.8.1** Security of electronic or paper copies of personal information;
 - 3.8.2** Security of online computer terminal(s);
 - 3.8.3** Designation of authorized users and assignment of access codes;
 - 3.8.4** Proposed audit and management control over access and dissemination of requested information;
 - 3.8.5** Authentication method used to access online computer terminal(s);
 - 3.8.6** Security of records, files, and systems; and,
 - 3.8.7** Descriptions of system support process including backup methods and frequencies.
- 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 Clause 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 within 24 hours of discovering any breach of personal information contained in 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 Purchaser believes or has reason to believe to have been lost or compromised;
 - 3.9.6** Notifying the State within 24 hours of 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 website privacy and security policies which is available for viewing at https://dps.mn.gov/divisions/dvs/forms-documents/Documents/Policy125-1000Security_Confidentiality.pdf; and
- 3.9.9** Agreeing that DVS Data shall not be transferred nor accessed outside the United States, electronically or otherwise.

4. Payment

Purchaser will pay the State for all services performed by the State under this contract as follows:

- The cost per record for custom data request records (1,000 or more records per month) is governed by Minnesota Statutes, section 168.327, subdivision 5b, which is subject to change.
- The cost per record for non-custom data request records (999 or less records per month) is governed by Minnesota Statutes, section 168.327, subdivision 1f, which is subject to change.

The State will invoice Purchaser, and Purchaser will remit payment 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/her successor:

Name: Jennifer McKenna, Legal Affairs Director
Address: 445 Minnesota Street, Suite 191
Saint Paul, MN 55101-5191
Telephone: (651) 201-7775
Email Address: dvs.dataservices@state.mn.us

The Purchaser's Authorized Representative is the following individual, or his/her 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: Marissa Medina
Address: 128 South Tryon Street, Suite 1000
Charlotte, NC 28202
Telephone: (704) 312-1661
Email Address: marissa.medina@passportinc.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:

- Intentional, willful, or negligent acts or omissions; or
- Actions that give rise to strict liability; or
- 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 United States Code Section 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 sections 13.08 and 13.09 and Title 18 United States Code Sections 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.

9. Publicity

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 section 16C.05, subdivision 5, the Purchaser's books, records, documents, and accounting procedures and practices 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 end of this Contract.

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

10.3. 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. 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.

13. Use of DVS Data

Pursuant to Title 18 United States Code Section 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:

Registered vehicle owner names and addresses will be used to mail delinquent parking notices on behalf of our clients who are government agencies.

Purchaser: Passport Labs, Inc.

Print Name: Sarah Ratcliffe

Signature: *Sarah Ratcliffe*

Title: Sr. Vice President, Products Date: 3/15/2022

**1. State Agency: Department of Public Safety;
Driver and Vehicle Services Division**

With delegated authority

Print Name: Pong Xiong
DocuSigned by: _____

Signature: *Pong Xiong*

Title: DVS Div. Director Date: 4/5/2022

2. Commissioner of Administration

As delegated to the Office of State Procurement

Print Name: _____
DocuSigned by: _____

Signature: *Sara Friedland*

Title: _____ Date: 4/11/2022

Admin ID: _____

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, 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

[State 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. *Username 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 (State)

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**

Policy Number: 125-1000a

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: _____

Exhibit B

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

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.**