WASHINGTON STATE DEPARTMENT OF LICENSING	**DATA LICENSING AGREEMENT BETWEEN DEPARTMENT OF LICENSING AND [ENTER RECIPIENT LEGAL NAME]**	**DOL Contract No. K___**

Contract

Contract start date	**Contract end date**	**Contract amount**
Start Date	End Date	Revenue, no maximum Cost Recovery Non-financial

Purpose

This data sharing Agreement establishes the terms, conditions, restrictions, requirements, and authorization for Recipient to receive Data services from DOL. This Agreement replaces and cancels DOL contract number K___.

Data Type

☐ Driving Record	☐ Aggregate driver data	☐ Protected Personal Information (CAT 3, 4)
☐ Vehicle	☐ Manufactured home	☐ Non-Protected Personal Information (CAT 1, 2)
☐ Vessel	☐ Other _____	

Recipient

Recipient Name		**Recipient UBI**
Address		
Contract Manager	**(Area code) Telephone**	**Email**
Compliance Manager	**(Area code) Telephone**	**Email**
Technical Contact (IT)	**(Area code) Telephone**	**Email**

Department of Licensing (DOL)

Department administration Data Management Office	**Division** Office of Equity, Performance and Accountability	
Address PO Box 2076 Olympia, WA 98507-2076		
Contract Manager	**(Area code) Telephone** (360) 902-3920	**Email** datacontracts@dol.wa.gov
Compliance Manager	**(Area code) Telephone** (360) 902-3920	**Email** datacontracts@dol.wa.gov

Attachments (when applicable)

This Agreement consists of the following attachment(s) and Exhibits(s) incorporated herein or by reference:

Attachment A, *Data Licensing Statement(s)*
Attachment B, *Privacy and Security Requirements*
Attachment C, *Subrecipients Requirements*
Attachment D, *Audit Requirements*
Exhibit A, *Non-Compliance Form*
Exhibit B, *Cyber Liability Insurance Mitigation Table*

The terms and conditions of this Agreement are an integration of the final, entire, and exclusive understanding between the Parties, superseding all previous agreements, writings, and communications, oral or otherwise, regarding the subject matter of this Agreement. This Agreement is effective upon execution by both Parties. The Parties signing below represent that they have read and understand this Agreement and have the authority to execute on behalf of their entity.

Recipient Signature **Date**	**DOL Signature** **Date**
PRINT Signatory's Name, Title	**Name, Title** Evelyne Lloyd Assistant Director, Administrative Services Division
E-Mail:	

TABLE OF CONTENTS

This data sharing Agreement (Agreement) is between the Washington State, Department of Licensing (DOL), and [Recipient Name] (Recipient). DOL and Recipient may each be referred to individually as Party, or jointly as Parties.

In consideration of the terms and conditions contained herein, the Parties hereby agree as follows:

BACKGROUND INFORMATION

1. PURPOSE

   The purpose of this Agreement is to establish the terms, conditions, and restrictions for DOL to provide Recipient a license to use Data and for establishing Recipient's safekeeping and Permissible Use requirements over such information. This Agreement ensures that information is provided, protected and used only for purposes authorized by federal and state law governing the release of Data.

   The scope of this Agreement only provides the Recipient with access and Permissible Use of Data; it does not establish an agency relationship or independent contractor relationship between DOL and the Recipient.

   This Agreement supersedes all previous agreements, authorizations, waivers and approvals. If the Recipient received additional authorizations or approvals, such as for Offshoring, under the previous agreement, it must reapply. Any corrective actions, Access Period suspensions, or other conditions placed on the Recipient under the previous agreement remain in full force and effect until the conditions are satisfied.

2. LEGAL AUTHORIZATION

   This Agreement is made in accordance with all federal and state laws and rules as applicable, including but not limited to:

   a) Driver Privacy Protection Act 18 USC Ch. 123
   b) Revised Codes of Washington (RCW) 46.22.010, 46.04.652, 46.04.209, 46.04.1615
   c) RCW 46.52.130 – For Abstracts of Driving Records, as applicable
   d) RCW 46.12.630 – For Lists of Vehicle Owners, as applicable
   e) Washington Administrative Code may also apply
   f) (Other authority that may be applicable)

   It is the responsibility of the Recipient to ensure that anyone accessing Protected Personal Information is familiar with the statutes, rules and contract requirements governing the use of Protected Personal Information, including all staff, contractors, Subrecipients and Subrecipient staff, to ensure the appropriate disclosure and use of Protected Personal Information.

3. DEFINITIONS

   As used throughout this Agreement, the following terms shall have the meanings set forth below. Most terms used throughout this Agreement are defined in RCWs 46.22.010, 46.04.652, 46.04.209, and 46.04.1615, and applicable WAC. If there is a conflict between the definitions in this Agreement and definitions appearing in the RCW or WAC, the RCW or WAC will take precedence.

   a) "Access Period" is a duration of time under the term of this Agreement when Recipient is granted access and use of Protected Personal Information.
   b) "Agent" means a representative, or representatives, of a Requester that is under contract with the Recipient or Subrecipient to request driving records on the Requester's behalf. "Agent" includes insurance pools established under RCW 48.62.031 of which the authorized Recipient is a member.
   c) "Attorney" means an attorney functioning in a legal capacity when obtaining or using vehicle or vessel owner information from a Recipient or Subrecipient.
   d) "Breach" or "Breaches" means an unauthorized acquisition, loss of control or exposure to an unauthorized person or business, or Misuse of Protected Personal Information. Ransomware and unauthorized Offshoring of Protected Personal Information are included in this definition.
   e) "Consumer Report" has the same meaning as in 15 U.S. Code § 1681a.
   f) "Customers" means those entities that the Recipient is providing services to using Protected Personal Information but is not receiving Protected Personal Information from the Recipient.

"Customers" does not include those entities receiving statistical reports.

g) "Data" means information provided to Recipient under this Agreement.
h) "Governmental Entity" means a federal agency, a state agency, board, commission, unit of local government, or quasi-governmental entities.
i) "Incident" means an event that confirms, or is reasonably thought to be, the unauthorized access to, or Misuse of, Protected Personal Information. Ransomware attacks are included in this definition.
j) "Independent Third Party" means any entity other than a member of the Recipient or any of its stockholders, or any entity controlled by or under common control with any of the stockholders or the company group.
k) "Misuse" means the access, disclosure or use of Protected Personal Information without the express, written authorization from DOL in a data sharing agreement. "Misuse" also includes a violation of any privacy requirement outlined this Agreement.
l) "Offshoring" means the electronic or hardcopy transmission, accessing, viewing, capturing images, storage, or processing of Protected Personal Information outside the United States.
m) "Permissible Use" means authorized or required uses as outlined in federal or state law, and authorized in this Agreement.
n) "Private Investigator" has the same meaning as RCW 18.165.010(11), or as licensed by other authority.
o) "Protected Personal Information" means collectively Personal Information and Identity Information, as defined by RCWs 46.04.209, 19.255.005 and 42.56.590, authorized for disclosure by the federal Driver Privacy Protection Act and state law.
p) "Requester" means an entity with an authorized Permissible Use to receive Protected Personal Information from DOL. A requester may be an Agent, Subrecipient or a Recipient.
q) "Statement of Compliance" means an annual statement signed by an executive of an organization attesting to the Recipient's full compliance with requirements in this Agreement.
r) "Subrecipient" means any entity outside your immediate organization that receives or has access to Protected Personal Information, including but not limited to subsidiaries, subcontractors, Requestors, or Agents.

SPECIAL TERMS AND CONDITIONS

4. AGREEMENT TERM

The term of this Agreement begins on [start date], and ends on October 31, 2025, unless terminated sooner or extended by mutual amendment as provided herein. This Agreement may be extended for any duration of time determined by DOL, but for no more than an additional five (5) years beyond the initial term.

Any waivers, additional approvals, etc., granted by DOL under this Agreement shall expire at the end of this Agreement and will not carry forward to any subsequent data sharing agreement.

5. GRANT OF LICENSE

Subject to the terms and conditions of this Agreement, DOL hereby grants Recipient with a limited non-transferable license to receive and use Data as solely permitted under this Agreement.

6. DATA OWNERSHIP

DOL retains sole and exclusive ownership of the Data. Nothing in this Agreement grants the Recipient any ownership interests in the Data.

7. DATA LICENSING STATEMENT

A Data Licensing Statement describes the responsibilities and process Recipient must use in order to request Data. The *Data Licensing Statement* is incorporated into this Agreement under Attachment A – *Data Licensing Statement*. *Data Licensing Statements* are established to specify the following information relative to this Agreement:

a) Type of Data provided,
b) The Permissible Use(s) for such Data,
c) Identify how Data is transmitted and, if applicable, File Layout or Interface Control Document (ICD),

d) Fees and payment information, as applicable, and
e) Other requirements or information as may be applicable.

The Parties may incorporate additional Data Licensing Statements into this Agreement by written amendment fully executed by both Parties. Each Data Licensing Statement is to be incorporated by using the same attachment reference letter (A) and then further marking it with sequential identifying numbers (A1, A2, A3 etc.).

8. TRANSMISSION OF DATA BETWEEN DOL AND RECIPIENT

The system requirements for the transmission of Data are at the discretion of DOL. DOL will use its best efforts to always maintain the availability of the system and provide notice of changes to the system. DOL reserves the right to make unilateral changes to the system, or how Data is transmitted, with written notification to the Recipient.

Each request for Data must include:

a) The Permissible Use code, if required in the Interface Control Document (ICD) or File Layout, and
b) If applicable, unique ID number for each Subrecipient or Customer.

The transmission of Data to the Recipient by DOL will be made in accordance with Attachment A – *Data Licensing Statement*.

9. PRIVACY AND SECURITY REQUIREMENTS

To the extent that Data provided pursuant to this Agreement includes Protected Personal Information:

a) Recipient shall safeguard all Protected Personal Information as set forth in Attachment B - *Privacy and Security Requirements*. Recipient agrees that it has a continuing obligation to comply with all federal and state laws, regulations, and security standards as enacted or revised over time, regarding Data protection, Breach, Data transmission, and restricted Permissible Uses of Protected Personal Information.

b) Recipient has an ongoing obligation to ensure all its personnel, contractors and Subrecipients fully understand and comply with all *Privacy and Security Requirements*.

10. DATA LINEAGE

When comingling Data containing Protected Personal Information with data from another source that matches the Data fields provided to the Recipient by DOL, Recipient must use methods, such as metadata, to identify which information originated from DOL and track the Data lineage. Such methods must also be applied to Protected Personal Information shared with Subrecipients, and for the purpose of adhering to the data disposal requirements in this Agreement.

If the Recipient is unable to track the lineage of Data containing Protected Personal Information, DOL will consider any Protected Personal Information matching the Data fields provided to the Recipient by DOL, subject to the audit, *Privacy and Security Requirements*, and Breach notification requirements.

11. PERMISSIBLE USE

11.1 Recipient may only use Data containing Protected Personal Information for the Permissible Uses as set forth in Attachment A – *Data Licensing Statement*. This Agreement does not constitute a release of Protected Personal Information for the Recipient's discretionary use. The Data may be accessed and used only as authorized herein, including internally for system maintenance and testing. Any other use not specifically authorized herein is strictly prohibited.

11.2 The Recipient may not use Data not meeting the definition of Protected Personal Information to discern, establish, or determine the identity of, or otherwise re-identify an individual without prior written approval of DOL.

11.3 In accordance with RCW 43.17.425 and Washington Executive Order 17-01, Recipient and Subrecipients are explicitly prohibited without limitation against sharing or using Data, including Protected Personal Information, for purposes of investigating, enforcing, cooperating with, or assisting in the investigation or enforcement of any federal or state regulation or surveillance programs or any other laws, rules, or policies that target Washington residents solely on the basis of race, religion, immigration, or citizenship status, or national or ethnic origin.

11.4 Any violation of the Permissible Use of the Data or RCW 43.17.425 is strictly prohibited and may be cause for immediate termination of this Agreement, as well as other possible civil and criminal penalties.

11.5 When prior Protected Personal Information received and retained by Recipient is refreshed with new Data, Recipient must refrain from using the older Protected Personal Information and must dispose of it, unless otherwise required by federal or state law or regulation. Recipient may only use, sell, distribute, and disseminate Protected Personal Information that is the most current Protected Personal Information received under this Agreement unless specifically waived by DOL.

11.6 Recipient shall further comply with all Permissible Use requirements set forth on Attachment B – *Privacy and Security Requirements*.

11.7 DOL may monitor and investigate the use and security of Protected Personal Information received by the Recipient or its Subrecipients through this Agreement. The Recipient has a duty to cooperate with DOL's investigation and ensure Subrecipient's cooperation with such investigations.

12. INCIDENT / BREACH NOTIFICATION

12.1 Recipient must notify DOL when it reasonably believes an Incident or Breach took place, including Incidents and Breaches occurring at a Subrecipient, when Protected Personal Information is involved, at each of the following:

DOL Help Desk, phone: (360) 902-0111,
DOL Compliance Manager, phone: (360) 902-3920, and
DOL Event Management, email: DOLEventMgmt@dol.wa.gov

Recipient must disclose the Incident or Breach to DOL prior to any public notification.

12.2 In addition to the above requirement to notify DOL, Recipient must also comply with all applicable laws that require the notification of individuals as required by RCW 42.56.590 or RCW 19.255.010, as applicable. Recipient must cooperate with DOL to help facilitate notification of all necessary individuals as determined by DOL or other legal authority. At DOL's discretion, Recipient may be required to directly perform notification requirements.

Recipient is responsible for all costs, including, but not limited to, notification and credit monitoring costs resulting from an Incident or Breach. This includes DOL's costs for responding to the Incident or Breach. Nothing herein prevents Recipient from requiring any Subrecipient from being responsible for all costs resulting from a Subrecipient's Incident or Breach.

For purposes of this provision, unauthorized disclosure includes the disclosure to any employees, personnel, or Agents of Recipient who do not have a direct business need to access the Protected Personal Information.

13. INCIDENT / BREACH RESPONSE

When Protected Personal Information is involved in a Breach or Incident, the Recipient has a duty to cooperate with DOL's investigation, which is a routine part of DOL's incident response plan, including Incidents and Breaches occurring at a Subrecipient. In response to any Incident or Breach, Recipient must:

a) Participate in the exchange of information related to the Incident or Breach,
b) Cooperate in the investigation of an Incident or Breach, and
c) Make personnel available to participate in DOL's incident response team.

DOL reserves the right to require Recipient to suspend the Subrecipient's Access Period, for any person or Subrecipient found to have experienced a Breach. The Access Period will remain suspended until DOL provides written approval to provide Protected Personal Information to that Subrecipient.

14. SUBRECIPIENTS

Prior to sharing Protected Personal Information with Subrecipients, Recipient must have a written Agreement with Subrecipient that meets the requirements, terms, and conditions, set forth on Attachment C – *Subrecipient Requirements*.

Recipient is responsible for the regular overseeing, managing, and testing of compliance for all Subrecipients. Subrecipient noncompliance to the required terms or conditions of this Agreement are equally borne by the Recipient.

15. PAYMENTS

This is a non-financial agreement.

OR

Recipient must pay the fees as set forth in Attachment A – *Data Licensing Statement*. Recipient shall make timely payments in full amount for all Data it receives in accordance with each invoice. In the event Recipient does not make timely payments in full, the unpaid debt may be subject to applicable interest as allowed by law and may also be forwarded to a collection agency if remained unpaid for greater than ninety (90) days.

DOL may suspend Recipient's Access Period for non-payment under this Agreement, or any other monies owed to DOL.

16. ADDITIONAL DATA RUNS OR RERUNS

Requests from Recipient for reruns or technical support at frequencies or dates not already agreed upon within this Agreement may require additional fees. Each additional Data run or rerun may be billed at actual amount for staff time to perform the work. Additional set up fees may also apply. "Rerun" means the re-delivery of a previous sent file unless there was a corruption or DOL error in the original file.

17. INSURANCE

A. Required Coverages

Recipient shall maintain self-insurance or commercial insurance as outlined herein. Insurance must be maintained with carriers that are authorized to do business in Washington State and maintain a minimum AM Best rating of A-: VII, or an equivalent rating with a similar rating agency.

All insurance must be primary to any other insurance programs afforded to or maintained by DOL or the state of Washington. Recipient waives all rights against DOL and the state of Washington for recovery of damages to the extent that such damages would be covered by general liability or umbrella insurance maintained by Recipient pursuant to this Agreement.

Recipient must notify DOL within thirty (30) days if a claim has been made under the commercial general liability or self-insurance policy related to the Data provided under this Agreement.

a) Commercial General Liability

Recipient shall maintain self-insurance, or a commercial general liability insurance policy, including contract liability, in adequate quantity to protect against legal liability arising out of activity from this Agreement. Policy shall not be less than the following:

- $1,000,000 per occurrence

- $2,000,000 aggregate

b) Professional Liability (Errors & Omissions)
Recipient shall maintain Professional Liability insurance covering errors, omissions, or negligence in the activities under this Agreement. Policy shall not be less than the following:
- $5,000,000 per occurrence
- $10,000,000 aggregate

c) Cyber Liability
If the Recipient is receiving Protected Personal Information from DOL, beginning January 1, 2024, the Recipient shall maintain cyber liability insurance with policy amounts as outlined below, based on the number of unique individuals' records containing Protected Personal Information in Recipient's possession on January 1 of the year evidence was submitted, and every 3 (three) years thereafter. This insurance shall include coverage for third party claims and losses including with respect to network risks (such as: data Breaches, transmission of virus/malicious code, unauthorized access or criminal use of third party, ID/data theft) and invasion of privacy regardless of the type of media involved in the loss of private information (such as: computers, paper files and records, or voice recorded tapes), covering collection, use, access, etc., of Protected Personal Information, direct liability, as well as contractual liability for violation of privacy policy, civil suits and sublimit for regulatory defense/indemnity for payment of fines and penalties.

Number of Records Containing Protected Personal Information Held per Policy Period	Policy Value	Policy Value with Mitigations
Greater than one million unique individuals	$100,000,000	$15,000,000
500,001 – 1,000,000 unique individuals	$50,000,000	$7,500,000
250,001 – 500,000 unique individuals	$25,000,000	$3,750,000
100,001 – 250,000 unique individuals	$15,000,000	$2,250,000
50,001 – 100,000 unique individuals	$5,000,000	$1,000,000
5,250 – 50,000 unique individuals	$1,000,000	$1,000,000
1 – 5,249 unique individuals	Policy not required	

DOL will accept the Policy Value with Mitigations when the Recipient demonstrates to DOL's satisfaction certain risk mitigations are in place as described in Exhibit B, *Cyber Liability Insurance Mitigation Table*.

Recipient must receive written approval from DOL showing DOL accepted the evidence and approved the policy value with mitigations. DOL will notify the Recipient in writing when insufficient evidence was submitted, and the Recipient may submit new evidence for DOL's consideration at least 30 days prior to expiration of the current policy. Recipient must obtain a policy with the required value within 60 days of being notified by DOL of the requirement.

The Recipient will not be permitted a policy value less-than the value with mitigations.

If at any time Recipient fails to maintain one or more risk mitigations during the policy period, DOL reserves the right to rescind the policy value with mitigations.

A Recipient who has access to funds in Washington State's Self Insured Liability Program is deemed to meet this requirement.

B. Additional Insureds
The policies shall include, or be endorsed to include the following provisions:

a) With the exception of Professional Liability insurance, the state of Washington shall be named as an additional insured, when available to the Recipient, to the full limits of liability purchased by the Recipient even if those limits of liability are in excess of those required by this Agreement.

b) The Recipient's insurance coverage shall be primary insurance and non-contributory with respect to all other available sources.

C. Notice of Cancellation
Recipient shall provide written notice thirty (30) days in advance of the cancellation of any insurance required hereunder.

D. Certificates of Insurance
Prior to receiving any Data, Recipient shall provide DOL a valid certificate or certificates of insurance demonstrating the fulfillment of all requirements herein.

Recipient will submit new or renewal certificates on a yearly basis during the term of this Agreement without a lapse in coverage. Certificates must be received within thirty (30) days following the issuance or renewal of any policies or at the direction by DOL to obtain a policy with limits prescribed in this Agreement.

Failure to provide DOL with the required Certificates of Insurance may result in immediate suspension of Access Period and may, at DOL's sole discretion, result in termination of this Agreement.

18. AUDITS
Recipient shall be subject to regular audits as set forth on Attachment D – *Audit Requirements* during the period it possesses Protected Personal Information. Corrective actions that were outstanding under a prior corrective action plan are incorporated into this Agreement.

By entering into this Agreement, Recipient acknowledges its obligation to provide DOL access to complete unredacted copies of audits and waives any protections under RCW 42.56.420 solely with respect to disclosing its audits to DOL under this Agreement. Failure to disclose audit reports to DOL will be considered a breach of this Contract and subject to termination.

Information obtained by DOL through the audit process, including the audit report, shall be handled as confidential information. DOL will internally only disclose information obtained during any audit on a need-to-know basis. Any external release of information will be in compliance with the provisions of Chapter 42.56 RCW, Public Records Act.

Pursuant to RCW 46.22.010, DOL is not responsible for the costs of the audit, and DOL will invoice Recipient for audit costs as outlined in Attachment D – *Audit Requirements.* DOL will provide the Recipient an estimate of DOL's audit costs prior to the initiation of the audit.

19. AUDIT NON-DISCLOSURE AGREEMENT
This Agreement serves as a non-disclosure agreement between the Parties with regard to information exchanged during an audit or annual Statement of Compliance to the extent that the information is protected under RCW 42.56.420 or other applicable law.

DOL will not sign a separate non-disclosure agreement as it pertains to the exchange of information under the terms and conditions of the Agreement.

20. ANNUAL STATEMENT OF COMPLIANCE
If the Recipient is receiving Protected Personal Information from DOL, Recipient must submit annual statements of compliance attesting to its compliance with the *Privacy and Security Requirements*, *Subrecipient Requirements*, and cyber liability insurance requirements in this Agreement for the period it possesses Protected Personal Information and has Subrecipients that possess Protected Personal Information.

Annual statements of compliance are due each year on [fill in date].

a) A Statement of Compliance is a written statement drafted by the Recipient, attesting to DOL that it

is in compliance with requirements in the Agreement. The Statement of Compliance is valid when signed by personnel authorized to bind the Recipient. After conducting a self-assessment:

i. If Recipient is meeting all *Privacy and Security Requirements*, *Subrecipient Requirements*, and cyber liability insurance requirements in this Agreement, then Recipient's statement must affirm that it is in compliance with all *Privacy and Security Requirements*, *Subrecipient Requirements,* and cyber liability insurance requirements in this Agreement.

ii. If the Recipient determines it is not fully compliant with all *Privacy and Security Requirements*, *Subrecipient Requirements*, and cyber liability insurance requirements of this Agreement, Recipient must submit a completed Exhibit A – *Non-Compliance Form*. DOL and Recipient will work together to determine the actions needed to correct all deficiencies noted in the form. Actions pertaining to correcting deficiencies in a Statement of Compliance will be handled as a corrective action plan as described in Attachment D – *Audit and Compliance Reviews.*

b) Corrective actions that were incomplete under prior annual statements of compliance are incorporated into this Agreement and will continue to be monitored by DOL to completion.

c) If Recipient is processing Data under 15 U.S.C. §1681b as part of a Consumer Report, the Statement of Compliance must attest to compliance with the Federal Trade Commission's Disposal Rule (Disposal of Consumer Report Information and Records, 16 C.F.R., §682.3).

Failure to provide the annual Statement of Compliance may result in the suspension of the Recipient's Access Period.

21. SUSPENSION OF ACCESS PERIOD

21.1 The Recipient's Access Period may be suspended at DOL's discretion for non-compliance with this Agreement. During any suspension of an Access Period, all other terms and conditions of this Agreement remain in effect. If the Recipient's Access Period is suspended, Recipient may not obtain additional Data from DOL or any other sources where the Protected Personal Information originates from DOL, nor may Recipient use or release any Protected Personal Information it has in its possession, except as required under RCW 46.12.630(1) until the suspension is lifted, or as otherwise required by law.

CHOOSE ONE OF THE FOLLOWING TWO OPTIONS:

Recipient's Access Period automatically begins with the execution of this Agreement. However, all conditions and corrective actions, if any, that were incomplete under the prior agreement are automatically forwarded and incorporated into this Agreement.

OR

Recipient's Access Period begins at such time as the Recipient demonstrates compliance with requirements set forth in this Agreement, including:

a) *Privacy and Security Requirements* outlined in Attachment B – *Privacy and Security Requirements*.

b) Other requirements or conditions as communicated to the Recipient by DOL in writing.

21.2 Recipient may only provide a Subrecipient with access to Protected Personal Information during Recipient's active Access Period. During the suspension, Recipient must notify the Subrecipients that they are prohibited from accessing and using Protected Personal Information.

21.3 Termination of Access Period.

The expiration or termination of this Agreement automatically terminates the Recipient's Access Period. Any suspension lasting longer than ninety (90) days may automatically terminate this Agreement under Section 22.3, *Termination for Cause*.

22. TERMINATION

Termination of this Agreement may be made as set forth below.

22.1 Unilateral Termination by Recipient

Recipient may terminate this Agreement at any time and for any reason upon providing written notice to DOL. If at the time of termination Recipient was under a corrective action plan or cure process, or had outstanding invoices, DOL may refuse future Agreements.

22.2 Administrative Terminations

If DOL's authority to actively engage in this Agreement is suspended or terminated, such a termination or suspension will automatically cause a termination or suspension of this Agreement. DOL is to provide as much notice as possible when such termination or suspension appears eminent.

Additionally, if DOL, as a state agency, determines that the continuation of this Agreement no longer conforms to DOL's policy, and/or is no longer in the best interests of DOL or the state of Washington, DOL may terminate this Agreement for convenience by giving written notice to the Recipient at least fifteen (15) business days before the effective date of termination. Administrative terminations are without cause.

Finally, if the Recipient has not received Data within the last twelve (12) months, DOL may administratively terminate this Agreement.

22.3 Termination for Cause

DOL may terminate this Agreement if Recipient or Recipient's Subrecipient violates a term, condition, or requirement of this Agreement. DOL has sole discretion on whether the Recipient or Subrecipient's non-compliance is cause for an immediate termination or suspension or whether the Recipient or Subrecipient should be given a cure process to correct the non-compliance.

For any determination of non-compliance, DOL must provide Recipient with a written statement identifying the full nature of Recipient's non-compliance. If DOL allows for a cure process, the Parties will work together to establish the process and timeline. DOL may suspend the Access Period to Data during a cure process. The agreed-upon cure process will be put in writing and acknowledged by both Parties. If Parties cannot mutually determine a cure process, or if Recipient does not substantially complete the cure process within the stated timelines, DOL then has the right to terminate this Agreement.

Any suspension lasting longer than ninety (90) days may lead to termination for cause.

22.4 Termination for Convenience

DOL may terminate this Agreement for convenience, upon thirty (30) days' written notice to the Recipient.

23. POST TERMINATION/SUSPENSION PROCEDURES

After receipt of a notice of termination or suspension, Recipient must immediately refrain from accessing, using, and disseminating any Data, except as allowed under RCW 46.12.630(1), or as otherwise directed by DOL in writing. Recipient must also settle all outstanding liabilities and claims arising from any pending or prior Data requests. Additionally, the Recipient must clear Protected Personal Information in accordance with Section 9, *Data and Media Sanitization*, of Attachment B – *Privacy and Security Requirements*.

24. CONFLICTS BETWEEN DOL DATA SHARING AGREEMENTS

If Recipient has multiple data sharing agreements with DOL, and if conflicts exist between those agreements as they relate to *Privacy and Security Requirements*, Recipient must adhere to the strictest of those requirements unless an exception to those requirements is specifically stated in this Agreement, or a written waiver has been granted by DOL.

25. PENALTIES

The unauthorized disclosure or use of Protected Personal Information is subject to civil and criminal

penalties pursuant to federal and state statutes.

26. ADDITIONAL DATA

If Recipient wishes to receive additional Data or wishes to use the current Data for Permissible Uses other than as authorized herein, Recipient must submit a new Data Records Contract Application for an amendment to this Agreement or a new data sharing agreement. If DOL agrees to provide the Data for the requested Permissible Uses or provide the additional data requested, then DOL will issue an amendment or a new agreement that contains the additional information, terms, and conditions. Such amendment or agreement will not be valid until properly executed by both Parties.

27. TECHNICAL REQUIREMENTS

Any disruption in Data delivery will be restored at a time determined by DOL.

The Recipient is responsible for the advance internal testing of Recipient's system in response to all DOL system changes, of which DOL will use its best efforts to provide advance notice, prior to the implementation of all DOL system changes.

28. FUNDING CONTINGENCY

In the event funding from state, federal or other sources is withdrawn, reduced, or limited in any way after the effective date of this Agreement and prior to normal completion, DOL may suspend this Agreement without advance notice. This Agreement may be subject to renegotiation under any new funding limitations and/or conditions.

29. REQUIREMENT WAIVER

DOL, in its sole discretion, may grant the Recipient a waiver to certain requirements outlined herein. The Recipient must apply for the waiver to DOL and supply all requested information, including a plan for how and when the Recipient will be in compliance with the requirement. DOL may require the Recipient to implement an action plan to ensure the Recipient's future compliance. The Waiver must be approved in writing and in advance of Recipient not meeting the requirement.

GENERAL TERMS AND CONDITIONS

30. AMENDMENTS

This Agreement may only be amended by mutual agreement of the Parties. Such amendments are not binding unless they are in writing and signed by personnel authorized to bind each of the Parties.

Only DOL's Director or designated delegate by writing has the expressed authority to alter, amend, modify, or waive any clause or condition of this Agreement. Furthermore, any alteration, amendment, modification, or waiver of any clause or condition of this Agreement is not effective or binding unless made in writing and signed by DOL's Director or delegate.

31. ASSIGNABILITY

If Recipient's ownership changes, it must provide written notice to DOL within thirty (30) days. DOL, in its sole discretion, will determine if the Agreement will be assigned, terminated, or a new agreement issued.

32. CONTRACT MANAGEMENT

The Recipient's contract manager, and DOL's contract manager, respectively listed on page one (1) are responsible for all official communications and notices pertaining to this Agreement. All such communications and notices are to be made between the respective managers unless alternative personnel are established for specific purposes. The use of email, to the most current email address on file for the other Party, is an acceptable form of providing notice for all purposes in this Agreement. Only written notifications will be accepted for official notices.

The Recipient must notify DOL in writing within thirty (30) calendar days of changes to: business name, ownership, business address, phone number, email address, or contract manager or his/her contact information.

33. COMPLIANCE MANAGEMENT

Recipient must designate a compliance manager who is responsible for assuring that Recipient complies with all reporting and *Privacy and Security Requirements*. If no compliance manager is named on the first page of this Agreement, or subsequently named thereafter, then the contract manager will be deemed the compliance manager.

34. DISPUTES

The Parties agree that time is of the essence in resolving disputes. The designated contract managers must use their best efforts to resolve disputes between the Parties at the lowest administrative level. If these individuals are unable to resolve the dispute, the responsible program directors of each party will review the matter and attempt resolution. This process shall not interfere with or prohibit DOL's ability to terminate this agreement for administrative, cause or convenience.

35. GOVERNANCE

This Agreement shall be construed and interpreted in accordance with the laws of the state of Washington and the venue of any action brought hereunder shall be in the Superior Court for Thurston County.

In the event of an inconsistency in this Agreement, unless otherwise provided, the inconsistency shall be resolved by giving precedence in the following order:

a) Applicable federal and Washington State laws, and regulations,
b) Terms and conditions of this Agreement, and
c) Any additional attachments or other material incorporated herein by written reference.

36. LEGAL FEES

Unless otherwise specified by law, and except as otherwise stated herein, in the event of litigation or other action brought to enforce Agreement terms, each Party shall bear its own legal fees and costs.

37. INDEMNIFICATION

Each Party, to the maximum extent allowed by law, shall defend, protect and hold harmless the other Party from and against all claims, suits or actions arising from either negligent or intentional acts or omissions, including Breaches, of the respective entity, and its Subrecipients, or Agents of the Recipient, while performing the terms of this Agreement.

38. INDEPENDENT CAPACITY

The scope of this Agreement only provides the Recipient with access and Permissible Use of Data; it does not establish an agency relationship or independent contractor relationship between DOL and the Recipient. Nothing herein may be deemed as allowing any employee or agent of one Party to be considered as the employee or agent of the other Party.

39. INTEGRITY OF DATA

DOL receives data from multiple sources. As such, Recipient shall not hold DOL liable for any errors which occur in the accuracy of Data.

If DOL has determined it has provided Data incorrectly or inappropriately to the Recipient, it may require the Recipient cease all use of, and clear the Data in accordance with Section 9, *Data and Media Sanitization,* of Attachment B - *Privacy and Security Requirements*. If the Recipient provided the Data to any Subrecipient, the same requirements may apply.

DOL may provide corrected information, if available, to the Recipient, which will also be available to the Subrecipient(s) where applicable.

40. NON-EXCLUSION OF REMEDIES

The rights and remedies of the Parties as provided in this Agreement, are not exclusive and are in addition to any other rights and legal remedies provided by law, including without limitation, the right to receive financial reimbursement for any incurred damages.

41. RECIPIENT LEGAL COMPLIANCE STANDARDS

Recipient must comply with all applicable local, state, and federal laws rules and regulations. Such compliance minimally includes without limitation, all applicable licensing requirements of the state of Washington, all civil rights and non-discrimination laws, the Americans with Disabilities Act (ADA) of 1990, and all federal and state employment laws. Failure to comply with this provision may be grounds for termination of this Agreement regardless of the affect it may have on the subject matter of this Agreement.

42. RECIPIENT PROPRIETARY INFORMATION

Recipient acknowledges DOL is subject to chapter 42.56 RCW, *Public Records Act*, and this Agreement is a public record as defined by that Act. Any confidential or proprietary information submitted to DOL must be clearly identified as such by the Recipient. To the extent consistent with chapter 42.56 RCW, DOL will maintain the confidentiality of all such information marked confidential or proprietary.

If a request is made for the Recipient's proprietary information and DOL intends to release the information, DOL will notify the Recipient of the request and notify the Recipient of the date records will be released to the requester. It will be the responsibility of the Recipient to obtain any necessary court order enjoining that disclosure by the stated release date. If the Recipient fails to obtain the court order enjoining disclosure, DOL will release the requested information.

If the Recipient is a Governmental Entity governed by other public disclosure laws, the Recipient must follow the applicable statutes. If the Recipient receives a request for any Protected Personal Information provided under this Agreement, and it does not have authority to redact the Protected Personal Information, it must notify the DOL contract manager prior to the Protected Personal Information being released.

43. PUBLICITY & MEDIA

The Recipient must get DOL's written consent prior to using DOL's name or logo, or Data on any business forms, advertising, or publicity where the name or logo are included or may be reasonably implied.

If DOL approves any advertising and publicity, DOL reserves the right to add a disclaimer and/or rescind its approval later. Recipient may not use the Washington State seal under any circumstance.

If the Recipient is the subject of a media article or story that includes DOL or its Data, it must notify the DOL contract manager immediately.

44. RECORDS ACCESS, INSPECTIONS AND MAINTENANCE

Recipient, at the request of DOL, must provide access to all records retained in connection with administration of this Agreement. Records include documentation regarding the management of this Agreement and excludes Data obtained over the term of the Agreement. Records inherently include access to all records under the Driver Privacy Protection Act. Recipient is to keep all records created in relation to this Agreement for no less-than six (6) years beyond the end of this Agreement, this includes without limitation:

a) Information pertaining to a Breach or Incident and the response to that Breach or Incident, for both Recipient and Subrecipients,
b) Communications of a substantial nature with Subrecipients about anything covered by Attachment C, *Subrecipient Requirements*,
c) Payments and refunds between Recipient and DOL as they pertain to actions under this Agreement,
d) Recipient audits, annual Statement of Compliance and supporting documentation, and

e) Subrecipient audit documentation, relating to the *Privacy and Security Requirements, Subrecipient Requirements*, compliance activities, and data sharing contracts.

When Protected Personal Information is shared with Subrecipients or Customers, Recipient must keep the following information for a period of five (5) years:

a) Name of each Subrecipient or Customer on whose behalf an individual record was obtained,
b) A unique ID number for each Subrecipient or Customer, for requests for driving records,
c) The total number of unique individuals' records the Subrecipient received in a calendar year; and
d) The Permissible Use of each record obtained.

All records subject to this section must be made available for inspection and review in non-redacted form regardless of any claim of privilege or confidentiality, except for attorney-client privilege. DOL may request copies at no additional cost to DOL. Recipient may designate some sections or pages as being confidential and/or privileged by noting such designation in writing. Recipient may provide a cover sheet listing all pages or sections that it considers privileged or confidential. DOL will maintain confidentiality over all such records to the extent allowed by law.

Recipient also agrees to work with DOL for purposes of obtaining necessary records from Subrecipients upon request.

If any litigation, claim, or audit is started before the expiration of the six-year period, the records must be retained until all litigation, claims, or audit findings involving the records have been resolved including any appeals and remands.

45. SEVERABILITY
If any term or condition of this Agreement is held invalid, the remainder of the Agreement remains valid and in full force and effect.

46. SURVIVORSHIP
The terms, conditions and warranties contained in this Agreement that concern, but are not limited to, privacy, record retention, audits, Annual Statements of Compliance, Access Period, insurance, destruction of Data, survive the completion of the performance, cancellation or termination of this Agreement, and remain in full force and affect until such time that all Protected Personal Information is surrendered and/or destroyed as set forth on Attachment B – *Privacy and Security Requirements*.

47. WAIVER
A failure by either Party to exercise its rights under this Agreement shall not preclude that Party from subsequent exercise of such rights and shall not constitute a waiver of any other rights under this Agreement unless stated to be such in a writing signed by an authorized representative of the Party and attached to the original Agreement.

DOL will insert applicable Data Licensing Statement determined by the data being requested.

ATTACHMENT B – PRIVACY AND SECURITY REQUIREMENTS

This attachment applies when the Recipient receives Protected Personal Information from DOL; it does not apply if the Recipient does not receive Protected Personal Information from DOL.

PRIVACY REQUIREMENTS

The Recipient must have a privacy framework. At a minimum, the framework must include principles and methodologies for identifying and managing privacy risks, including the following.

1. PRIVACY POLICY
   Recipient must have a privacy policy that:
   a) Declares data is managed as an asset of the organization, and outlines appropriate controls for the protection of data, and
   b) Sets an expectation that all personnel will secure, use, and dispose Protected Personal Information in alignment with Recipient's privacy and security practices, which must collectively align with these Privacy Requirements.

2. PRIVACY NOTICE
   Recipient must have a privacy notice available to inform the public how Recipient gathers, shares, uses, discloses, and manages Protected Personal Information.

3. INCIDENT RESPONSE PLAN
   Recipients are required to have an incident response plan to respond to an Incident or Breach involving Protected Personal Information. At a minimum, the plan is to include:
   a) Procedures the Recipient uses to prepare for, detect, respond to, and recover from Incidents or Breaches,
   b) Notification to DOL; and
   c) Notification in accordance with chapter 19.255 RCW or RCW 42.56.590.

4. PRIVACY IN SYSTEM DEVELOPMENT, OPERATION AND MAINTENANCE
   The Recipient must have and use a process to consider the impacts to the privacy of Protected Personal Information when developing systems, products, new versions of existing products, and services. Commonly known as "privacy by design."

5. TRAINING
   The Recipient must train its personnel, including contractors, with access to Protected Personal Information on its privacy policy.

DOL may update these Privacy Requirements as may be required by state policy or law.

DATA SECURITY REQUIREMENTS – ELECTRONIC RECORDS - external

All Protected Personal Information in ELECTRONIC FORM must be secured as follows:

The Recipient must protect Protected Personal Information with administrative, technical and physical measures that meet generally recognized cyber security industry standards and best practices, including those established by the Washington State Office of the Chief Information Officer (OCIO). Examples of acceptable cyber security industry standards and best practices include:

- ISO 27002,
- PCI DSS,
- NIST 800 series, and
- OCIO Policy 141.10.

DOL will audit to the standards in OCIO Policy 141.10 when Recipient does not have an industry standard acceptable to DOL in place to secure electronic information.

The Recipient must meet the following minimum standard requirements for securing Protected Personal Information. Recipient's controls for each topic must align with the selected industry standard or as otherwise required by DOL below:

1. NETWORK SECURITY – Recipient must:
    a) Use a network firewall that protects in-scope systems from untrusted networks,
    b) An intrusion detection system or techniques that detect and or prevent intrusions on the in-scope network, and
    c) Perform quarterly vulnerability assessments and annual penetration tests.

2. ACCESS SECURITY – Recipient must have active user authentication, that at minimum:
    a) Uses a unique user ID and complex password,
    b) Passwords changed on a periodic basis (at least quarterly), and
    c) Prohibits the use of generic and shared accounts.

3. APPLICATION SECURITY
    a) Recipient shall maintain in-scope systems receive software and subsequent upgrades, updates, patches, and bug fixes that must, at minimum, be maintained and supported such that the software is at all times secure from known vulnerabilities ranked "High" or above.
    b) All web applications must minimally meet all the security controls as generally described in either
        i. The Open Web Application Security Project Top Ten (OWASP Top 10), or
        ii. The CWE/SANS TOP 25 Most Dangerous Software Errors

4. COMPUTER SECURITY – Recipient must:
    a) Maintain in-scope operating systems, and software updates and patches, no less than monthly so they each remain secure from known vulnerabilities ranked "High" or above, and
    b) Have an active anti-malware solution with signatures updated no less than weekly.

5. DATA STORAGE
    a) Recipient must maintain a list of all in-scope computing systems storing, processing, or transmitting Protected Personal Information.
    b) Protected Personal Information may not at any time be processed on or transferred to any detachable portable storage medium.
        i. NOTE: Laptop/tablet computing devices are not considered portable storage medium when installed with end-point encryption.

6. ELECTRONIC DATA TRANSMISSION
   Recipient must secure all internal and external electronic data transmissions of Protected Personal Information with strong encryption.

7. DATA AT REST
   Recipient must encrypt Protected Personal Information while at rest with strong encryption.

8. DATA MINIMIZATION
   Recipient must have a policy for the retention of Protected Personal Information. Recipient must only retain Protected Personal Information for the duration of time needed to fulfill the Permissible Use for which it was obtained, as well as any legal requirements to retain the record for the minimum required retention period.

   Recipient may request a written waiver pursuant to Section 29 – *Requirement Waiver*. The request must include:
    a) The reason and business need for retaining the Protected Personal Information,
    b) An explanation of how the request aligns with federal or state retention laws (with specific citation of each law referenced),

c) An explanation of any litigation holds, if applicable,
d) An action plan for when Recipient will comply with this requirement,
e) The schedule for destruction, and
f) The effective end date for the waiver.

9. DATA AND MEDIA SANITIZATION
Recipient must have a data and media sanitization policy that aligns with current guidelines and definitions in NIST SP 800-88, to include:
a) "Clear" or "clearing" applies when removing Protected Personal Information from media once the Protected Personal Information has met the retention policy required in Section 8, *Data Minimization*, of this attachment, or as directed by DOL.
b) "Purge" or "purging" applies when removing Protected Personal Information from media when media are reused for purposes within the organization but will not store Protected Personal Information.
c) "Destroy" or "destroying" applies when removing media that stored Protected Personal Information when the media is not going to be reused by the organization.

Unless explicitly required by law, Recipient must provide one or more certificates of Clearing Protected Personal Information, Purging Protected Personal Information from media, or Destroying media storing Protected Personal Information, within thirty (30) days of:
a) Written request by DOL, or
b) Termination of this Agreement.

DATA SECURITY REQUIREMENTS – HARD COPY RECORDS

The Recipient must secure all Protected Personal Information in hard copy form as follows:

1. HARD COPY STORAGE
Printed copies must be stored in locked containers or storage areas when not in use by authorized persons. Examples include a physically secure workspace, locked cabinets, or vaults. Hard copy documents must never be unattended or in areas accessible to the public.

2. HARD COPY TRANSPORTATION
a) Hard copy documents containing Protected Personal Information taken outside a secure area must be in the possession of an authorized person, or a trusted courier providing tracking services.
b) Records must be maintained for all transported hard copies showing the person(s)/courier(s) responsible for such transportation, including the receiving party.

DATA SECURITY REQUIREMENTS – OFFSHORING

1. OFFSHORING – ELECTRONIC RECORDS
a) Recipient must maintain the primary, backup, disaster recovery and other sites for processing or storage of Protected Personal Information only from locations in the United States.
b) Recipient may not, without advance written approval from DOL:
i. Directly or indirectly (including through Subrecipients) transmit Protected Personal Information outside the United States, or
ii. Allow access to Protected Personal Information from outside the United States.

2. OFFSHORING – HARD COPY
a) Recipient must maintain all hard copies containing Protected Personal Information at locations in the United States.
b) Recipient may not directly or indirectly (including through Subrecipients) transport any Protected Personal Information outside the United States unless it has advance written approval from DOL.

PERMISSIBLE USE REQUIREMENTS

1. DATA USE AND TRAINING
   Recipient must institute and maintain written policies to ensure Protected Personal Information is only used as authorized herein. At a minimum, the policies must address training for all personnel with access to Protected Personal Information. Training must include:
   a) Permissible Use(s) of Protected Personal Information as authorized in the Agreement,
   b) Limitations on Permissible Use(s) of Protected Personal Information that prohibit the use of Protected Personal Information for anything other than authorized in the Agreement,
   c) Penalties for Breach of Protected Personal Information, and
   d) Identifying and reporting an Incident or Breach of Protected Personal Information.

2. PERMISSIBLE USE
   Recipient must verify its use and disclosure of the Protected Personal Information is in accordance with the Permissible Use(s) established in this Agreement.

3. MONITORING PERSONNEL
   Recipient must implement administrative, technical, or physical methods to monitor personnel for compliance with the Permissible Use(s) authorized in this Agreement across all business practices. Methods must address monitoring access to, and use of, Protected Personal Information**.**

ATTACHMENT C - SUBRECIPIENT REQUIREMENTS

The Recipient must apply these Subrecipient Requirements to any Subrecipient that receives Protected Personal Information directly from the Recipient in the following order.

1. SUBRECIPIENT POLICY AND PROCEDURES
   Prior to disclosing any Protected Personal Information to a Subrecipient, the Recipient must adopt policies and procedures to effectively:
   a) Implement the controls required in these Subrecipient Requirements, and
   b) Ensure that all Subrecipients follow all Privacy and Security, Subrecipient and Audit Requirements outlined in this Agreement.

2. REQUIRED VETTING OF SUBRECIPIENTS
   Prior to providing Protected Personal Information to any Subrecipient, Recipient must have a process to ensure that the Subrecipient is a Legitimate Business per WAC 308-10-010 and has an authorized Permissible Use according to this Agreement. Recipient has an on-going obligation to ensure Subrecipients maintain the qualifications allowing them access to the Protected Personal Information.

3. CONTRACT WITH SUBRECIPIENT
   Prior to providing or continuing to provide Protected Personal Information to a Subrecipient, Recipient must have a written contract with the Subrecipient that incorporates this Agreement into the Subrecipient Contract so that the Subrecipient is fully aware and subject to DOL's requirements when handling and processing Protected Personal Information. Upon request, DOL will provide a sample contract attachment the Recipient can use to satisfy this requirement.

   The Subrecipient contract must:
   a) Include a statement that DOL retains sole and exclusive ownership of the Data. Nothing in the agreement may convey or grant the Subrecipient any ownership interest in the Data,
   b) Inform the Subrecipient its access to Data may be suspended should DOL suspend or limit Recipient's access to or use of Protected Personal Information, and while access is suspended, the Subrecipient must cease from using any Data in its possession,
   c) State the specific Permissible Use(s) of the Data provided to the Subrecipient, with a statement the Data can be used for no other purpose unless otherwise required by law,
   d) Require Recipient be notified when Subrecipient experiences an Incident or Breach, or reasonably believes an Incident or Breach of Protected Personal Information took place, and the Recipient must notify DOL of the Incident or Breach,
   e) Require Subrecipients that annually receive fewer than 5,250 unique individual's records containing Protected Personal Information, to take all wjfxtsfgqj%xjhzwy~%uwthjizwjx%fsi%uwfhyhjx necessary to prevent the unauthorized disclosure and Misuse of Protected Personal Information,
   f) For Subrecipients that annually receive 5,250 or more unique individual's records containing Protected Personal Information, pass on all *Privacy and Security Requirements* in Attachment B through to all Subrecipients receiving Protected Personal Information originating from DOL,
   g) As applicable, for vehicle or vessel owner information, require the Subrecipient to provide notice where appropriate to the vehicle or vessel owner whenever the Subrecipient discloses Protected Personal Information of a vehicle or vessel owner to an Attorney or Private Investigator, and
   h) As applicable, require the Subrecipient to obtain prior written consent from the Requester before requesting a Driving Record for employment/prospective employment or volunteer organizations. At a minimum, the consent form must conform to and contain the required content under CONSENT REQUIREMENTS in Attachment A-1 – *Data Licensing Statement for Abstract of Driving Records*.

4. SUBRECIPIENT NON-DISCLOSURE AGREEMENTS
Recipient shall not enter into non-disclosure agreements with Subrecipients that prohibit or bar DOL from knowing who receives Protected Personal Information, and how the Protected Personal Information is used. Additionally, Recipient shall not enter into a non-disclosure agreement with a Subrecipient preventing DOL from being notified of Breaches, or from accessing all information needed, in DOL's sole discretion, regarding the facts of the Breach.

5. LIMITED ACCESS AND USE
Recipient must have controls to limit Subrecipient access to Protected Personal Information for only uses authorized in the Subrecipient contract.

6. COMPLIANCE

A. For Subrecipients annually receiving less than 5,250 unique individual's records containing Protected Personal Information, the Recipient must ensure that the Subrecipient take all reasonable actions necessary to prevent the unauthorized disclosure and Misuse of Protected Personal Information.

B. For Subrecipients annually receiving 5,250 or more unique individual's records containing Protected Personal Information:

a) Recipient must have procedures to regularly audit all Subrecipient(s), as applicable, for compliance with the requirements in Attachment A – *Data Licensing Statement(s)*.

b) Recipient must have procedures to regularly audit all Subrecipient(s) for compliance with the requirements the *Privacy and Security Requirements* in Attachment B, as passed through in the Subrecipient's data sharing agreement with the Recipient. Recipient may accept third-party audits conducted within the past 12 months. The audits must determine Subrecipient's compliance with the *Privacy and Security Requirements* when the Subrecipient retains the Protected Personal Information.

Nothing herein shall prevent Recipient from requiring that a Subrecipient be responsible for all such costs of an audit.

C. If the Recipient finds a Subrecipient to be non-compliant with applicable requirements through the process of conducting audits, it must either:

a) Ensure that non-compliance is corrected within a reasonable timeframe, or

b) Suspend or terminate Subrecipient's access and use of Protected Personal Information.

7. SUBRECIPIENT LIST
When requested by DOL, Recipient must provide a list of names, and the respective Permissible Uses, for all the entities defined as Subrecipients and Customers. This list must be provided in Excel format or may be provided in another format at DOL's discretion, without redactions. The list must be provided within ten (10) business days of written request by DOL, and no less than annually.

The list at a minimum, must contain the following information:

a) Recipient name,

b) Date of the list,

c) All Subrecipient and Customer names, with their respective trade (doing business as) names,

d) Unique ID number for each entity requesting a driving record, as applicable,

e) Entity type (e.g., insurance company, employer, transit, governmental, etc., and for vehicle or vessel owner information only, if the entity was an Attorney or Private Investigator),

f) If the entity is Offshoring Protected Personal Information, and if so, to where and for what Permissible Use,

g) Whether the entity receives and processes Protected Personal Information (versus Recipient processing Protected Personal Information on the entity's behalf),

h) A count of the number of DOL records obtained in the past year, and
i) Permissible Use(s) for which records are requested, as authorized in this Agreement.

Recipient must keep the list for a minimum of five (5) years.

8. SUBRECIPIENT DISQUALIFICATION
If DOL notifies Recipient that it has disqualified a Subrecipient from receiving Protected Personal Information, Recipient must immediately terminate and prevent the Subrecipient's access and use of Protected Personal Information.

9. OFFSHORING BY SUBRECIPIENT
Recipient must not allow any Subrecipient to Offshore Protected Personal Information unless Recipient obtains permission for Subrecipient to do so.

1. AUDIT AUTHORITY
   Audits are required when DOL provides Data containing Protected Personal Information, pursuant to RCW 46.22.010.

2. AUDIT SCOPE AND CRITERIA
   a) Data Security audits will address one or more of the following areas of this Agreement:
      i. Privacy Requirements in Attachment B
      ii. Data Security Requirements in Attachment B
      iii. Terms and conditions of this Agreement
   b) Permissible Use audits will address one or more of the following areas of this Agreement:
      i. Privacy Requirements in Attachment B
      ii. Permissible Use Requirements in Attachment B
      iii. Subrecipient Requirements in Attachment C
      iv. Terms and conditions of this Agreement
   c) Consent form audits will address one or more of the following areas of this Agreement when Recipient obtains Data requiring consent from the named individual.
      i. Data Licensing Statement(s) in Attachment A
      ii. Subrecipient Requirements in Attachment C

3. AUDIT OBJECTIVES
   To determine if:
   a) Recipient has adequate internal controls (policies, procedures, monitoring, etc.) in place to provide reasonable assurance that requirements in scope are achieved.
   b) The internal controls are operationalized and effective.
   c) Recipient materially complies with Agreement requirements.

4. AUDIT REQUIREMENTS

	Data Security Audits	**Permissible Use Audits**	**Consent Audits, as applicable**
Due Date or Timeline	• Recipient must obtain and provide a complete audit report and submit it to DOL before receiving Data under this Agreement. The completed audit report must be submitted to DOL no later than one year following the full execution date of this Agreement.	• Set by DOL • DOL will provide a minimum three (3) months' advance notice of an audit date.	• Set by DOL • DOL will provide a minimum three (3) months' advance notice of an audit date.

	• DOL may consider Data Security audits performed in the previous twelve (12) months. • Extensions may be granted due to conditions beyond the control of the Recipient. o A written request for an extension must be submitted in advance of the due date. o The request must describe the work done to-date to produce the audit and demonstrate progress toward delivering an audit report.		
Audit Cycle	• At DOL's discretion. • The standard cycle is one audit every three (3) years, measured from the due date of any prior audit report. • At DOL's discretion, audits can be required outside the three-year audit cycle when DOL has reason to suspect that the Recipient is in non-compliance with this Agreement. • Exceptions to the standard may be granted; in such cases, no less than one audit every four (4) years, measured from the due date of any prior audit report.	• At DOL's discretion. • The standard cycle is one audit every three (3) years, measured from the due date of any prior audit. • At DOL's discretion, audits can be required outside the three-year audit cycle when DOL has reason to suspect that the Recipient is in non-compliance with this Agreement. • Exceptions to the standard may be granted; in such cases, no less than one audit every four (4) years, measured from the date any prior audit was conducted.	• At DOL's discretion.
Audit Standards	• The engagement package is based on attestation standards established by the American Institute of Certified Public Accountants and Government Auditing Standards issued by the Comptroller General of the United States, • State agencies that must comply with the Office of the Chief Information Officer (OCIO) Policy 141, Securing Information Technology Assets, may benefit from audits conducted using audit standards developed and published by the Washington State Auditor's Office (SAO), or • Agreed upon procedures for DOL audits published by the Washington State Auditor's Office (SAO).	• Audit process and procedures developed by DOL; to be shared in advance of the audit.	• Audit process and procedures developed by DOL; to be shared in advance of the audit.
Auditor Qualification and Selection	• Auditors must meet the auditor qualifications as determined by DOL. • Audits must be conducted by DOL, or Independent Third-Party auditors selected by the Recipient.	DOL or its designated agent will perform all Permissible Use audits.	DOL or its designated agent will perform all consent audits.

	• Recipient is responsible to select the Independent Third-Party auditor. DOL may make available qualified audit firms.		
Cost of Audit	• Recipient is responsible for all costs associated with data security audits, including: o Independent Third-Party auditors o DOL staff labor when coordinating, scheduling, receiving, and reviewing the audit, to the point the final audit review is published. o If Recipient chooses to use a third-party auditor provided by DOL, Recipient must prepay the estimated audit costs to DOL. If the actual cost of the audit differs in amount from the amount prepaid, DOL will reimburse or invoice Recipient the difference. o All travel expenses of DOL personnel when conducting the audit in-person, including per diem. • DOL will notify Recipient in advance when DOL's costs of performing or reviewing the audit will exceed $50,000.	• Recipient is responsible for all costs associated with permissible use audits, including: o Independent Third-Party auditors o DOL staff labor when coordinating scheduling, and conducting the audit; and, drafting and reviewing the audit report, to the point the final report is published by DOL. An estimate will be provided prior to the audit. o All travel expenses of DOL personnel when conducting the audit in-person, including per diem. • DOL will notify Recipient in advance when costs of performing or reviewing the audit will exceed $50,000.	• Recipient is responsible for all costs associated with consent audits, including: o DOL staff labor when coordinating scheduling, and conducting the audit; and, drafting and reviewing the audit report, to the point the final report is published by DOL. An estimate will be provided prior to the audit. o An agent of DOL's choosing. o All travel expenses of DOL personnel or its agent when conducting the audit in-person, including per diem. • DOL will notify Recipient in advance when costs of performing or reviewing the audit will exceed $50,000.
DOL Audit Invoice	Recipient must make final payment within thirty (30) days of receiving a DOL invoice for audit costs.		
Audit Terms	• An exception is a situation where DOL identified a condition making it possible for it to conclude the Recipient is not in full compliance with a requirement. • A material weakness in internal control is defined as a deficiency, or combination of deficiencies, in internal control over compliance such that there is a reasonable possibility that material noncompliance with the requirements in this Agreement, would not be prevented, or detected and corrected, on a timely basis. • A significant deficiency is defined as a deficiency, or a combination of deficiencies, in internal control over compliance that is less severe than a material weakness in internal control over compliance, yet important enough to merit attention by those charged with governance.		
Audit Results	• Results will be formally communicated to Recipient by the DOL auditor noting all exceptions, including any significant deficiency or material weakness in internal control, noncompliance with this Agreement, laws or regulations, or abuse that come to the auditor's attention while conducting the engagement. • For Data Security Audits performed by auditors provided by DOL, and Permissible Use Audits, Recipient will have an opportunity to provide a management response, which would be added to the final report delivered to, or issued by, DOL. • A corrective action plan will be published with a final audit review or report when exceptions are identified.		
Corrective Action Plans	• Are required for all exceptions identified in an audit or annual Statement of Compliance. • Within a timeframe acceptable to DOL, Recipient must submit a corrective action plan for each exception identified by the audit or annual Statement of Compliance. For each exception, the corrective action plan must outline the deliverable to correct the deficiency, and a timeline for completing all corrective actions.		

- DOL will determine whether Recipient is substantially complying with the corrective action plan. If Recipient is not in substantial compliance, then DOL may suspend access to the Data or take other actions as allowed in this Agreement.
- Incomplete corrective actions under prior audits or annual statements of compliance are incorporated into this Agreement and will continue to be monitored by DOL to completion.

NON-COMPLIANCE FORM

This *Non-Compliance Form* must be completed by the Recipient during the annual internal assessment process outlined in Section 20, *Annual Statement of Compliance*, when it determines that it cannot comply with any component of the *Privacy and Security* or *Subrecipient Requirements*. The form must detail each component that is not in compliance.

Recipient Name:

Contact Person for additional information:

1. Standard(s) to which a deviation is requested:
   Section #:

2. Describe the reason for non-compliance or deviation with the standard:

3. Provide the business or technical justification:

4. Describe the scope including quantification and requested duration (normally not to exceed one year):

5. Describe all associated risks:

6. Describe any supplemental controls to mitigate risks resulting from the deviation.

7. Include a plan, with schedule, to achieve compliance with the IT security or Permissible Use standard(s):

8. Identify any unmitigated risks:

I have evaluated the business issues associated with this request and I accept any and all associated risks as being reasonable under the circumstances until compliance is achieved.

Recipient Signature _____ Date _____

For security reasons, submit only hard copy *Non-Compliance Form* or upload document to DOL via a secure file transfer method. Do not submit this form via unsecure methods.

To be offered the Policy Value with Mitigations, Recipient will use the following steps.

When Recipient provides evidence pertaining to Policy Value with Mitigations, Recipient must submit the number of unique individuals' records containing Protected Personal Information that Recipient holds as of January 1 on the year that evidence is submitted.

Step 1 - Disposal Options – select one of the following options for clearing[2] Protected Personal Information from your systems.

Select	Option	Information is Disposed of:	Number of Mitigations Required
☐	A	within 36 months of receipt	Three of the six options in Step 2
☐	B	within 84 months of receipt	Four of the six options in Step 2
☐	C	beyond 84 months of receipt	Five of the six options in Step 2

See Detail of Disposal Options for more information.

Step 2 – Mitigation Options – Choose mitigations from the following list. The number of mitigations selected must align with your preferred option in Step 1.

Select	#	Mitigations
☐	1	Data security and privacy policies
☐	2	Annual data security and privacy training
☐	3	Annual cyber security audits
☐	4	Annual security risk assessment
☐	5	Data retention and disposal policies
☐	6	Security and privacy governance

See Detail of Mitigation Options for more information.

Detail of Clearing Options

Option	Clearing Option	Examples of Evidence Needed
A or B	Dispose of all Protected Personal Information within selected timeframe.	A statement attesting to disposal signed by personnel authorized to bind the Recipient.
C	Holds Protected Personal Information for more than 84 months.	A statement attesting to holding information for more than 84 months, signed by personnel authorized to bind the Recipient.

Detail of Mitigation Options – The mitigations outlined below cover some of the same security and privacy subjects listed in Attachment B – *Privacy and Security Requirements*. Note that these risk mitigations exceed the requirements in Attachment B – *Privacy and Security Requirements*.

#	Mitigation Detail	Examples of Evidence Needed
1	Comprehensive Data security and privacy policies are adopted and founded on a recognized cybersecurity and privacy framework. The cybersecurity framework must be one of the following:	1. Adopted policies where the policy identifies the cybersecurity and privacy frameworks used as the foundation of the policies, and 2. Adopted policies remain in effect.

	1. WA Office of the Chief Information Officer, or 2. On the IT Governance list of top cybersecurity frameworks (https://www.itgovernanceusa.com/blog/top-4-cybersecurity-frameworks). The privacy framework must be one of the following: 1. WA Office of Privacy and Data Protection, 2. NIST Privacy Framework, or 3. ISO 27701	
2	Annual Data security and privacy training provided to all personnel processing Protected Personal Information. All personnel processing Protected Personal Information must take annual security and privacy training. Training must have content on acceptable use of confidential information, penalties for the misuse of confidential information, proper handling of confidential information, and securing confidential information.	Produce an excerpt of material showing the required content on Data security and privacy training, along with evidence of annual training on a sample population of personnel.
3	Conduct annual cyber security audits on systems processing DOL Data. Audits must meet the audit standards in Attachment D, *Audit Requirements*.	1. Cover sheet of annual audit on systems processing Protected Personal Information and disclosure of any exceptions noted in the audit, and 2. Information must be provided to demonstrate the audit meets the audit standards in Attachment D, Audit Requirements.
4	Annual security risk assessment Assessment is conducted using a recognized framework. The framework must appear on a list of top cybersecurity frameworks identified above under item 2. An action plan must be in place for all high or critical findings.	1. An adopted policy committing organization to the cybersecurity framework, 2. The policy is current and in effect, 3. Coversheet of annual assessment, and 4. The status of all high or critical findings.
5	Data retention and disposal policies regarding confidential information are in effect and not outdated. Policies must be current and no more than five years since they were last updated, adopted, or reviewed. Records must show the policies are in effect. Policies must align with the applicable Clearing Option in Step 1.	1. Coversheet and version control information on policies, and 2. Evidence of actual disposal, or clearing, of Protected Personal Information in accordance with the policies.
6	Security and Privacy Governance Recipient has a full-time qualified chief information security officer (or equivalent) AND a qualified chief privacy officer (or equivalent) on staff. A person holding either role can serve in other security or privacy roles with the Recipient. A person appointed to fill the role on an acting basis is acceptable to DOL.	Evidence each position is filled.

	A vacancy more than three consecutive months is equal to not having the role filled for the year.	