DocuSign Envelope ID: C49B1468-594E-4B9D-AA8E-D743D6E08BBD

WASHINGTON STATE DEPARTMENT OF LICENSING

DATA LICENSING AGREEMENT AMENDMENT BETWEEN DEPARTMENT OF LICENSING AND WASHINGTON STATE UNIVERSITY TRANSPORTATION SERVICES

DOL Contract No. K7786
Amendment No. 01

Contract

Contract start date	Contract end date	Contract amount for this Amendment
Upon Execution	October 31, 2025	Revenue, no maximum

Purpose
This Amendment updates Section 17. Insurance, Section 20. Annual Statement of Compliance and adds Exhibit B – Cyber Liability Insurance Mitigation Table.

Data Type for this Amendment, if applicable

☐ 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
Washington State University, Transportation Services		
Address		
1040 NE Colorado St, Pullman, WA 99164-5500		
Contract Manager	**(Area code) Telephone**	**Email**
Cody Wilson	(509) 335-0523	cody.wilson@wsu.edu
Compliance Manager	**(Area code) Telephone**	**Email**
Cody Wilson	(509) 335-0523	cody.wilson@wsu.edu
Technical Contact (IT)	**(Area code) Telephone**	**Email**
Aaron Colyar	(509) 335-4397	acolyar@wsu.edu

Department of Licensing (DOL)

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

Amendment

The Parties hereby agree to amend the Agreement as set forth below:

Updates Section 17. Insurance with revised cyber liability insurance requirements.

Updates Section 20. Annual Statement of Compliance to include attestation for cyber liability insurance requirements.

Adds 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
DocuSigned by: Amanda Owen 5EE9B9B0E6AE432...	9/25/2023	DocuSigned by: Evelyne Lloyd A530C5CAB0E2465...	9/26/2023
PRINT Signatory's Name, Title		**Name, Title**	
Amanda Owen, Associate Director		Evelyne Lloyd Assistant Director, Administrative Services Division	
E-Mail: amanda.owen2@wsu.edu			

DS

DocuSign Envelope ID: C49B1468-594E-4B9D-AA8E-D743D6E08BBD

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) 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

DocuSign Envelope ID: C49B1468-594E-4B9D-AA8E-D743D6E08BBD

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.

DocuSign Envelope ID: C49B1468-594E-4B9D-AA8E-D743D6E08BBD

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 June 1.

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.

DocuSign Envelope ID: C49B1468-594E-4B9D-AA8E-D743D6E08BBD

EXHIBIT B – CYBER LIABILITY INSURANCE MITIGATION TABLE

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. WA Office of the Chief Information Officer, or 2. On the IT Governance list of top cybersecurity frameworks	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.

	(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.	1. 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 Mitigation Detail number 2 (two). 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 Mitigation Detail number 1 (one).	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. A vacancy more than three consecutive months is equal to not having the role filled for the year.	1. Evidence each position is filled.