WASHINGTON STATE DEPARTMENT OF LICENSING

Driver and Plate Search (DAPS) and Driver Information and Adjudication System (DIAS) Agency Access Request

Please read before completing the attached form to request access to the DAPS or DIAS (formerly IHPS) systems.

- **DAPS** – online driver and vehicle records search for use in investigations used by law enforcement, courts, prosecuting attorneys, and governmental agencies.
- **DIAS** – online system to view and electronically update driver records used by courts, prosecuting attorneys, and governmental agencies.

An executive with the authority to authorize the **Account Administrator** to contractually bind your agency for system access must sign the form. A copy of documentation that identifies the administrator as an employee of your agency (examples: employee ID, credentials, badge, etc.) is also required. Once the access request is approved, the **Account Administrator** will be required to create a License eXpress for business account and sign a click-to-agree Interagency Data Sharing Agreement for Driver and Vehicle System (DRIVES) Access ("Agreement").

Once the account is set-up, the Account Administrator will be able to add **Managers** to manage user access to the system.

It is important that you read and understand the Agreement's terms and conditions. Here is a link to the Agreement **https://www.dol.wa.gov/external/daps-dias.html** and below are some key points. Please refer to the Agreement for complete requirements:

- You will manage access of your Authorized Users in DRIVES. Their roles and responsibilities will be:
  - **Administrator** has the designated authority from your organization to click to agree on the Agreement. They will be the person responsible for administering this Agreement, and for managing all Manager and User accounts on behalf of the Licensee. The Administrator has the capability to:
    - Perform authorized functions consistent with permissions granted by DOL;
    - Request codes to add Managers and Users;
    - Revoke Manager and User access; and
    - View and search activities performed by all Authorized Users.
  - **Managers** have the capability to:
    - Perform authorized functions consistent with permissions granted by DOL;
    - Request codes to add other Managers and Users;
    - Revoke Manager and User access; and
    - View and search activities performed by all Authorized Users.
  - **Users** have the capability to:
    - Perform authorized functions consistent with permissions granted by DOL; and
    - View and search their activities.
- Each authorized user must have an individual License eXpress account.
- Access must be revoked immediately when it is no longer required for job responsibilities.
- Governmental agencies can use the data for performing their job functions, except pursuant to Executive Order 17-01, DOL data may not be used for purposes of investigating, locating, or apprehending individuals for immigration related violations.
- You must proactively ensure that information access through DAPS and/or DIAS is only used as allowed by the Agreement, and notify DOL immediately of any misuse.
- You must conduct annual assessments for Data Security, Permissible Use and Internal Control requirements of this Agreement and annually attest to DOL that you meet these requirements.

WASHINGTON STATE DEPARTMENT OF LICENSING

Driver and Plate Search (DAPS) and Driver Information and Adjudication System (DIAS) Agency Access Request

Agencies use this form to request access to the DAPS or DIAS systems. A person with authority to commit its organization to contractual obligations must sign this form.

Email the completed application and documentation that identifies the designated contract administrator as an employee of your agency *(examples: employee ID, credentials, badge, etc.)* to: **DataServices@dol.wa.gov**

Online system access *(select all that apply)*:

☑ DAPS – online driver and vehicle records search for use in investigations

☐ DIAS – online system to view and electronically update driver records used by courts, prosecuting attorneys, and government agencies.

Agency name Redmond Police Department	
ORI or NCIC number WA0171200	EIN, TIN, or UBI
Office name and location Redmond Police, MSPSPD	
Physical address *(Street, Apartment or suite number, City, State, ZIP code)* 8701 160 Ave Ne, Redmond Wa 98073	
Mailing address *(Address or PO Box, City State, ZIP code)* 8701 160 Ave Ne, PO Box 9710, Redmond Wa, 98073-9710	
Account administrator name (person authorized to agree to the click-through contract) Robert Clemmons	Title 911 Communications Supervisor
Email rclemmons@redmond.gov	(Area code) Telephone number (425) 556-2652

Provide a detailed explanation of why you need driver or vehicle record information. Insufficient detail or specifics may cause your application to be rejected.

To assist the Redmond Police Department's enforcement and investigation duties.

Will you disclose the information to third parties? ..... ☐ Yes ☑ No

If "Yes," to whom and why? Be specific.

Do you have the authority to delegate the account administrator named above to agree to the contract terms and conditions? ..... ☑ Yes ☐ No

I certify under penalty of perjury under the laws of the state of Washington that the foregoing is true and correct.

8/28/18
Date and place signed

X [signature]
Signature (Type your name or sign here)

for John Marchione, Mayor — Malia Files, Finance Director
Title

For office use only

Date received _____ ☐ DIAS ☐ DAPS Action taken: ☐ Approved ☐ Denied

DSHS child support enforcement? ☐ Yes ☐ No

911 dispatchers? ☐ Yes ☐ No

X _____
Signature of approver

DSC-425-009 (R/9/18)WA

INTERAGENCY DATA SHARING AGREEMENT
FOR DRIVER AND VEHICLE SYSTEM (DRIVES) ACCESS

The agreed upon Terms and Conditions herein establish a Data Sharing Agreement (hereinafter "Agreement") between the Washington State Department of Licensing (hereinafter "DOL"), and the governmental agency named on DOL's Driver and Vehicle System (DRIVES) Access Account (hereinafter "Licensee"). DOL and Licensee may be individually referred to as "Party", or collectively referred to as "Parties."

Pursuant to the mutual terms and conditions herein, and based upon Licensee agreement hereto by clicking on the "Agree" button, the Parties hereby agree as follows:

1. BACKGROUND AND PURPOSE

In accordance with the Revised Code of Washington (RCW), government agencies may have the right to access and receive specific information maintained by the Department of Licensing as contained in vehicle and/or driver records. This information may be accessed through DRIVES, at DOL's discretion.

The purpose of this Agreement is to provide the terms and conditions for authorizing governmental entities to access DRIVES.

2. LEGAL JUSTIFICATION

The Data shared under this Agreement is permitted pursuant to the following authority: chapters 39.34, 42.56, 46.12, and 46.52 RCW; chapter 308-10 Washington Administrative Code (WAC); and/or the Federal Driver Privacy Protection Act (DPPA) 18 U.S.C. §2721 through §2725.

3. DEFINITIONS

As used throughout this Agreement, the following terms have the meanings set forth below:

"**Authorized Users**" means those authorized by the Licensee to access Data under this Agreement. Authorized users include Administrators, Managers and Users.

"**Confidential Information**" means information that may be exempt from disclosure to the public or other unauthorized persons under either chapter 42.56 RCW or other state or federal statutes and data defined as more sensitive than "public" and requires security protection. Confidential Information includes, but is not limited to, vehicle legal owner, social security numbers, credit card information, driver license numbers, Personal Information, law enforcement records, agency security data, and banking profiles.

"**Data**" means information obtained from DRIVES and provided to Licensee. This definition inherently includes material that contains Confidential Information.

"**Data Security**" means defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. This applies regardless of the form the Data may take (electronic, physical, etc.).

"**Data Security Breach**" means unauthorized acquisition of Confidential Information that compromises the security, confidentiality, or integrity of Confidential Information maintained by the person or business as defined in RCW 19.255.010.

"**Permissible Use**" means only those uses authorized in this Agreement and as specifically

defined.

"**Personal Information**" means information identifiable to any person, including, but not limited to information that relates to a person's name, health, finances, education, business, use or receipt of governmental services or other activities, addresses (except 5-digit zip code), telephone numbers, social security numbers, driver license numbers, e-mail addresses, credit card information, law enforcement records or other identifying numbers or Protected Health Information, any financial identifiers, and other information that may be exempt from disclosure to the public or other unauthorized persons under either RCW 42.56.360, chapter 42.56 RCW, or other state and federal statutes.

"**Subrecipient**" means any secondary or subsequent entity who receives the Data from the Licensee or through a chain of entities originating with the Licensee. Pursuant to RCW 46.52.130, this may include an employer or prospective employer, an insurance carrier; transit authority, or volunteer organization and their respective agents.

SPECIAL TERMS AND CONDITIONS

4. TERM OF AGREEMENT

The term of this Agreement begins on the date Licensee accepts the terms of this Agreement. The initial end term of this Agreement is for five (5) years, however, DOL may extend this Agreement for additional three-year terms simply by allowing the Licensee to maintain its use of this service.

5. GRANT OF LICENSE

Subject to the terms and conditions of this Agreement, DOL hereby grants Licensee with a limited non-transferable license to have access to selected DOL vehicle, vessel, and/or driver Data available through DRIVES.

This grant of access does not provide Licensee with any ownership rights to the Data; at all times DOL remains the sole owner of the Data.

6. ACCESS TO DATA

Each individual who will be accessing Data on behalf of the Licensee through DRIVES must set up an individual License eXpress account. All account transactions will be monitored by DRIVES to identify the information accessed through each of Licensee's accounts. Licensee must immediately revoke the access of any Authorized User when such access is no longer required.

If a specific User Account is dormant for over a year, DOL has the right to terminate such account. If all User Accounts are dormant for over a year, DOL has the right to terminate this entire Agreement.

Licensee must actively monitor access and use of Data by Authorized Users to ensure Data is accessed or used only for official job responsibilities. Licensee must immediately revoke the access of any Authorized User who accesses or uses Data without a Permissible Use. DOL also reserves the right so suspend or terminate the access of specific users if DOL determines that such user is not maintaining compliance with this Agreement.

Authorized User accounts are not interchangeable and cannot be shared; only the identified established person for any account may use that account. All Authorized Users must have an individual account, which is authorized by an Administrator or Manager.

The use of computerized applications (such as "bots") to access, retrieve, or store Data is prohibited.

A. ADMINISTRATOR

Licensee first must designate an Administrator. The Administrator will be the person responsible for administering this Agreement, and for managing all Manager and User accounts on behalf of the Licensee. The Administrator has the capability to:

- Perform authorized functions consistent with permissions granted by DOL;
- Add Managers and Users;
- Revoke Manager and User access; and
- View and search activities performed by all Authorized Users.

B. MANAGERS

Managers have the capability to:

- Perform authorized functions consistent with permissions granted by DOL;
- Request codes to add other Managers and Users;
- Revoke Manager and User access; and
- View and search activities performed by all Authorized Users.

C. USERS

Users have the capability to:

- Perform authorized functions consistent with permissions granted by DOL; and
- View and search activities performed for self.

7. DATA SECURITY AND SAFEGUARDING

Data provided pursuant to this Agreement may include public, Personal and Confidential Information. Licensee acknowledges and 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 Security, electronic data interchange and restricted uses of such information. Licensee further agrees that is has and shall maintain a privacy policy that has practices and procedures complying with these standards.

Licensee shall further protect and safeguard all Confidential Information against any and all unauthorized disclosure, use, or loss as set forth in Attachment A - *Data Security Requirements*.

At no time shall the Licensee or its employee or agent use, divulge, disclose, release, or communicate any Confidential Information to any individuals or entities, or for any purposes, outside the scope of specific Permissible Uses allowed by this Agreement.

8. SECURITY BREACH NOTIFICATION

Licensee shall comply with all applicable laws that require the notification of individuals in the event of unauthorized release of Data or other event requiring notification. In the event of a breach of any of Licensee's security obligations, or other event requiring notification under applicable law, Licensee must perform the following:

a) Notify DOL by telephone and e-mail of such an event within 24 hours of discovery:
DOL Help Desk, phone: (360) 902-0111,
DOL Help Desk, email: hlbhelp@dol.wa.gov

b) Cooperate and facilitate with the notification of all necessary individuals. At DOL's discretion, Licensee may be required to directly perform notification requirements, or if DOL elects to perform the notifications, Licensee may have to reimburse DOL for all costs associated with the notification.

9. PERMISSIBLE USE

Data may only be used for lawful actions related to the Licensee's functions as a governmental agency, and as directly related to the purposes set forth in Licensee's application, and as approved by DOL. All other use of Data is strictly prohibited. DOL further retains the right to re-determine its approval for permitted uses and may cancel or restrict such uses at a later date if such uses do not comply with state law or DOL policy. If any purposes noted in the application are otherwise restricted by any terms of this Agreement, then the restrictions herein are controlling. This prohibition on certain uses includes, without limitation, the use of Data for purposes of investigating, locating, or apprehending individuals for immigration related violations.

In addition to maintaining the Permissible Uses herein, Licensee shall also comply with all requirements set forth on Attachment B – *Permissible Use Requirements*.

10. SUBRECIPIENTS

Licensee may not provide Data containing Personal Information to any additional entities (Subrecipients) without first obtaining written permission by DOL. If any Personal Information is provided to a Subrecipient, the Licensee must forward all terms and conditions herein onto the Subrecipient. Licensee will remain responsible for the Subrecipient's full compliance with all terms and conditions herein.

11. INTERNAL CONTROLS

Licensee is responsible for ensuring that Authorized Users fully understand and abide by all terms and conditions of this Agreement; inherent in this requirement is that Licensee must institute proper training and disciplinary measures.

Licensee is strictly responsible for all actions of its Authorized Users, employees and agents in connection with the accessing of Personal Information under this Agreement.

If Licensee determines that an Authorized User has accessed or used Data for any purpose beyond what is authorized in this Agreement, pursuant to Attachment B – *Permissible Use Requirements*. DOL may deny access to any Authorized User who violates any provision of this Agreement.

12. ANNUAL SELF-ASSESSMENT

Licensee shall self-assess its own entity to determine whether it is properly complying with the Data Security, Permissible Use and Internal Control requirements of this Agreement. At a minimum, the assessment must including the following:

a) A yearly evaluation to determine if Licensee is in compliance with the Data Security Requirements as set forth in Attachment A – *Data Security Requirements*;

b) A yearly evaluation to determine if Licensee is compliance with the Permissible Use Requirements set forth in Attachment B – *Permissible Use Requirements*;

c) All Authorized User accesses have been revoked immediately when such access is no longer required;

d) All Data Security Breaches and Permissible Use violations have been made known to DOL in a timely manner; and

e) All Data has been disposed of in a timely manner and as set forth in Attachment A – *Data Security Requirements*.

Upon request by DOL, Licensee must provide DOL with a written certification acknowledging the completion of an assessment.

If the assessment determines that Licensee is meeting all requirements outlined above, then Licensee's certification may simply note that the assessment was completed and no deficiencies were found. However, if deficiencies are discovered, Licensee must disclose all deficiencies by submitting a completed form, which will be provided by DOL. DOL and Licensee will then work together to determine the final actions needed in order to correct all deficiencies.

Failure to submit the certification upon DOL's request or failure to correct deficiencies may result in DOL terminating this Agreement.

The written certification must be executed by a manager, director, or officer of Licensee who has the expressed signatory authority to make such a certification on behalf of Licensee.

13. AUDITS

DOL may request information and perform random audits on Licensee to verify its full compliance with the terms and conditions of this Agreement, and further to verify the accuracy of Licensee's self-assessment. Inherent in this right, DOL may review any independent, third-party Data Security or Permissible Use audit performed on the Licensee within the last three years as it pertains to Data accessed from DOL. Based on assessment findings, and on additional information gained by DOL, DOL may request that Licensee obtain further independent audits, and/or engage in specific corrective action to cure deficiencies.

If Licensee believes that any information given to DOL for these purposes is confidential or privileged information, Licensee may mark such information accordingly. Subject to the provisions of chapter 42.56 RCW (Public Records Act), which applies to all state and local agencies, DOL will maintain the confidentiality of such information, and will provide Licensee with all notifications and protection rights afforded by the Public Records Act.

Licensee is responsible for all costs related to audits and corrective actions.

GENERAL TERMS AND CONDITIONS

14. ALTERATIONS AND AMENDMENTS

This Agreement may only be amended by further mutual agreement of the Parties. Such amendments will be posted in DRIVES by DOL, and Licensee's Administrator will approve such amendment through electronic verification.

15. COMPENSATION

This is a non-financial Contract and there are no costs to be charged to Licensee.

16. CONTRACT COMMUNICATIONS AND NOTICES

The Administrator is responsible for all general communications and notices pertaining to this Agreement on behalf of Licensee. Additional personnel may be identified for established specific purposes. If no additional people are named, then the Administrator will be the default reference person for all communications.

The use of email to the most current email address of the Administrator is an acceptable form of providing communication and notice for all purposes in this Agreement.

Licensee is responsible to notify DOL in writing of any changes concerning the Administrator's name, phone number, or email address. Licensee may contact DOL contract manager at DataServices@dol.wa.gov.

17. CONTRACT DISPUTE RESOLUTION

The Parties agree that time is of the essence when initiating the contract dispute resolution process. All disputes should be first resolved at the managerial level between the two entities. If internal management and or executive leadership cannot resolve the dispute, then the Parties agree to use the alternative dispute resolution process as follows:

The Dispute Resolution Process will be initiated as follows:

- Be in writing;
- State the disputed issues;
- State the relative positions of the Parties;
- Be mailed to other Party's contract manager within three (3) business days after the Parties agree that they cannot resolve the dispute.

During the resolution process the Parties agree that:

- If the subject of the discourse is the payment DOL will continue performance and Licensee will pay the amount that it in good faith believes to be due and payable.
- If the subject of the discourse is not the payment due, DOL will continue performance of work under this Agreement that is not affected by the dispute.

The responding Party shall have ten (10) business days to respond in writing to the requesting Party's statement.

The initiating Party shall then review the written statements of the responding Party and reply in writing within ten (10) business days

Final determination of the Dispute will be done by the DOL Contracts Office, and will be final and conclusive unless, within five (5) business days from the date the Party receives such determination that Party requests a dispute panel in writing.

If a dispute panel is requested, DOL and Licensee will each appoint a member to the dispute panel within five (5) business days. DOL and Licensee will jointly appoint a third member to the dispute panel, within the next five (5) business days.

The dispute panel will review the written descriptions of the dispute, gather additional information as needed, and make a decision on the dispute in twenty (20) calendar days. The majority decision will prevail. The Parties agree that the decision of the dispute panel will be final and binding.

18. GOVERNANCE

This Agreement is governed by the laws of the state of Washington and any applicable federal laws. Venue for any legal action arising out of this Agreement is the Thurston County Superior Court.

In the event of an inconsistency in terms of this Agreement, or between the terms and any applicable statute or rule, the inconsistency will be resolved by giving precedence in the following order:

1. Applicable federal and Washington State laws, and regulations;
2. Specific Terms and conditions of this Agreement;

3. General Terms and conditions of this Agreement;
4. Attachments to this Agreement in sequential order; and
5. Any other documents and agreements incorporated herein.

19. INDEPENDENT CAPACITY

The scope of this Agreement maintains each Party's independent status as a self-governed entity, and 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.

20. INTEGRITY OF DATA

DOL compiles its Data based in part on the reporting of information from outside individuals and entities; as such, DOL may not be held liable for any errors which occur in compilation of Data. DOL may not be held liable for any delays in furnishing amended Data. DOL will make best efforts to ensure DRIVES is available. However, DOL makes no guarantee of system availability, accuracy of data, or that the Data will meet the Licensee's needs. DOL may make changes to DRIVES at any time to suit its business needs, without notification to Licensee.

21. INTERIM DISPOSAL OF DATA CONTAINING PERSONAL INFORMATION

Notwithstanding any permanent Data Disposal requirements set forth in Attachment A - *Data Security Requirements*, Licensee shall intermittently dispose of any Data containing Confidential Information at any time when Licensee's immediate use of that Data is no longer needed. Licensee is a government agency, and the Parties have mutually determined that the Licensee shall adhere to its required retention schedule.

22. RECORD MAINTENANCE

The Parties shall maintain all records relating to this Agreement, including all service and account records. All records and other material must be retained for six (6) years after expiration or termination of this Agreement.

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

23. RECORDS ACCESS AND INSPECTIONS

Licensee, at the request of DOL, must provide access to all records retained in connection with the receipt of Confidential Information under this Agreement. Upon request, such records must be made available for inspection, review, and/or copying at no additional cost to DOL.

24. RECORDS REQUEST – PUBLIC RECORDS ACT

Both Parties to this Agreement are subject to the chapter 46.52 RCW (Public Records Act). If Licensee believes that any information it gives to DOL is confidential or privileged in nature, then Licensee may mark such information accordingly. Subject to the provisions of the Public Records Act, DOL will maintain the confidentiality of such information, and will provide Licensee with all notifications and protection rights afforded by the Act.

If Licensee receives a public records request relating to any Confidential Information accessed under this Agreement, Licensee will maintain the full confidential nature of such information to

the greatest extent allowed by law. Licensee will further provide notice to DOL consistent with the requirements of the Public Records Act, and will fully support DOL in maintaining the confidential nature of such information.

25. HOLD HARMLESS

Licensee shall hold DOL harmless for any damages or claims arising from its own acts and/or omissions, which includes those acts or omissions of its Authorized Users, employees or agents.

26. SEVERABILITY

If any provision of this Agreement or any provision of any document incorporated by reference shall be held invalid, such invalidity shall not affect the other provisions of this Agreement which can be given effect without the invalid provision, if such remainder conforms to the requirements of applicable law and the fundamental purpose of this Agreement, and to this end the provisions of this Agreement are declared to be severable.

27. TERMINATION

Termination of this Agreement may be as set forth below. All termination matters may be applied as a suspension instead of a full termination, except that any suspension lasting longer than ninety (90) days will automatically terminate this Agreement.

A. Unilateral Termination by Licensee
Licensee may terminate this Agreement at any time and for any reason upon providing written notice to DOL.

B. Administrative Terminations
If DOL's authority to actively engage in this Agreement is suspended or terminated, whether by lack of funding, or by any other governmental issue, including internal changes in policy, that causes the disruption of authority to engage in the required activity, such a termination or suspension of authority will automatically cause a termination or suspension of this Agreement. DOL also retains the right to terminate this Agreement for convenience. DOL is to provide as much notice as possible when such termination or suspension appears eminent. This involuntary termination is without cause.

C. Termination for Cause
DOL's may terminate this Agreement, or any access privileges under this Agreement, for the violation of a material term or condition of this Agreement. DOL has sole discretion on whether such non-compliance is cause for immediate termination of the entire Agreement, whether it should suspend or terminate an Authorized User's access, or whether Licensee should be granted a cure process to correct any non-compliance without further actions.

28. WAIVER

The omission of either Party to exercise its rights under this Agreement does not preclude that Party from subsequent exercising of such rights and does not constitute a waiver of any rights under this Agreement, unless stated as such in writing, and signed by an authorized representative of the Party.

Attachment A
Data Security Requirements

1. DATA CLASSIFICATION

The classification of the Data shared under this Agreement includes:

- ☐ Category 1 – Public Information
- ☐ Category 2 – Sensitive Information
- ☒ Category 3 – Confidential Information (includes Personal Information)
- ☒ Category 4 – Confidential Information Requiring Special Handling (if Social Security Numbers, or medical information are provided)

For all Confidential Data that is electronically stored, processed, or transmitted, Licensee shall apply the following requirements:

2. DATA SECURITY

Licensee must protect the confidentiality, integrity and availability of Data with administrative, technical and physical measures that meet generally recognized industry standards and best practices or standards established by the Washington State Office of the Chief Information Officer (OCIO).

Examples of industry standards and best practices include any of the following:

a) **ISO 27002**
b) **PCI DSS**
c) **NIST 800 series**
d) OCIO 141.10 (**https://ocio.wa.gov/policies/141-securing-information-technology-assets/14110-securing-information-technology-assets**)

NOTE: DOL has the right to implement security measures that may exceed OCIO or industry standards and best practices; if any security measures of this Agreement exceed OCIO or industry standards and best practices, then the higher DOL measures will apply. However, if any security measures of this Agreement fall below OCIO standards, then OCIO standards will apply.

3. NETWORK SECURITY

Licensee's network security must include the following:

a) Network firewall provisioning
b) Intrusion detection
c) Quarterly vulnerability assessments
d) Annual penetration tests.

4. ACCESS SECURITY

Licensee shall restrict Authorized User access to the Data by requiring a login using a unique user ID and complex password or other authentication mechanism which provides equal or greater security. Passwords must be changed on a periodic basis at least quarterly. The sharing of user ID and passwords is strictly prohibited. Licensee is solely responsible for protection of all of its user IDs and passwords, and is responsible for all breaches caused through the use of its user IDs and passwords.

5. APPLICATION SECURITY

Licensee shall maintain and support its software and subsequent upgrades, updates, patches, and bug fixes such that the software is, and remains secure from known vulnerabilities. Licensee must secure web applications that minimally meet all the security controls as generally described in either:

a) The Open Web Application Security Project Top Ten (OWASP Top 10), or
b) The CWE/SANS TOP 25 Most Dangerous Software Errors

6. COMPUTER SECURITY

Licensee shall maintain computers that access Data by ensuring the operating system and software are updated and patched monthly, such that they remain secure from known vulnerabilities. Licensee computer device(s) must also be installed with an Anti-Malware solution and signatures updated no less than monthly.

7. DATA STORAGE

Licensee shall designate and be able to identify all computing equipment, on which Licensee stores, processes, and maintains Data. No Data at any time may be processed on or transferred to any portable storage medium. Laptop/tablet computing devices are not considered portable storage medium in this context provided it is installed with end-point encryption.

8. ELECTRONIC DATA TRANSMISSION

Licensee shall maintain secure means (e.g., HTTPS or SFTP) for the electronic transmission or exchange of system and application data with DOL or any other authorized Licensee.

9. DATA ENCRYPTION

Licensee shall encrypt all Data, whether in transit or at rest, by using only NIST or ISO approved encryption algorithms; this includes all back-up copies of Data. Licensee further must install any laptop/notebook computing device, processing Data, with end-point encryption (i.e., full disk encryption).

10. DISTRIBUTION OF DATA

Licensee may only use and exchange Confidential Information for the purposes as expressly described and allowed in this Agreement. In addition to any other restrictions on Permissible Use, Confidential Information may not be distributed, repurposed or shared across other applications, environments, or business units of Licensee. Licensee must assure that no Confidential Information of any kind is transmitted, exchanged or otherwise passed to other contractors/vendors or interested parties except Licensee and/or Subrecipients who have an authorized legal Permissible Use according to this Agreement, and who are under contract with Licensee.

11. DATA DISPOSAL

Unless a more immediate disposal requirement is set forth in this Agreement, Licensee, upon termination of this Agreement, shall erase, destroy, and render unrecoverable all DOL Confidential Data and certify in writing that these actions have been completed within thirty (30) days of the termination of this Agreement. At a minimum, media sanitization is to be performed according to the standards enumerated by NIST SP 800-88r1 Guidelines for Media Sanitization.

12. OFFSHORING - ELECTRONIC

Licensee must maintain the primary, backup, disaster recovery and other sites for storage of Confidential Data only from locations in the United States.

Licensee may not commit the following unless it has advance written approval from DOL:

a) Directly or indirectly (including through Subrecipients) transmit any Confidential Data outside the United States; or
b) Allow any Confidential Data to be accessed by Subrecipients from locations outside of

the United States.

For all Confidential Data that is physically stored, processed, or distributed in a hardcopy format, Licensee shall apply the following requirements:

13. HARDCOPY STORAGE

To prevent unauthorized access to printed Confidential Information obtained under this Agreement, and loss of, or unauthorized access to this Confidential Information, printed copies must be stored in locked containers or storage areas, e.g. cabinets or vaults. Hard copy documents must never be unattended or in areas accessible to the public, especially after business hours.

14. HARDCOPY TRANSPORTATION

If hard copy documents containing Confidential Information are taken outside a secure area, those documents must be physically kept in possession of an authorized person, or a trusted courier providing tracking services. Records must be maintained for all transported hardcopies showing the person(s)/courier(s) responsible for such transportation, including the receiving party.

15. OFFSHORING - HARDCOPY

Licensee must maintain all hardcopies containing Confidential Information at locations in the United States.

Licensee may not directly or indirectly (including through Subrecipients) transport any Confidential Information outside the United States unless it has advance written approval from DOL.

Attachment B
Permissible Use Requirements

1. **DATA USE**
   Licensee must institute and maintain written policies and procedures to ensure Data is only used as authorized herein. At a minimum the policies and procedures will include, training requirements for all personnel with access to Confidential Information on the Permissible Use(s) of Data. Licensee must be capable of demonstrating the training and education was delivered to all applicable personnel who have are an Authorized User, employees and agents.

2. **APPROPRIATE USE DECLARATION**
   Licensee must require all Authorized Users to sign an Appropriate Use Declaration prior to accessing DRIVES. The Declaration must include a statement that the Authorized User understands and acknowledges:
   1. His/her obligations and responsibility to use Confidential Information only to accomplish his/her official job duties;
   2. He/she will maintain the confidentiality and privacy of the information accessed;
   3. He/she will not share Confidential Information with unauthorized persons;
   4. He/she will not use Data access for personal reasons or benefit; and
   5. Misuse of any Confidential Information may be considered a felony and may be punishable by fine or imprisonment.

   Licensee must maintain the signed declaration. Licensee must provide copies of signed Appropriate Use Declaration upon request by DOL.

3. **PERMISSIBLE USE EVALUATIONS**
   At least annually, Licensee must conduct a review of all Authorized Users' access and use of Confidential Information to ensure that such access and use is within official job duties.

4. **SECURE USE**
   Licensee must maintain and support administrative, technical or physical methods used to monitor compliance with the Permissible Use(s) authorized in this Agreement across all Licensee business practices. Methods may include any of the following:
   a) View only access to Data
   b) System limitations or controls
   c) Confidentiality agreements

5. **NON-CONFORMING PERMISSIBLE USE NOTIFICATION**
   Licensee shall notify DOL personnel in the event of confirmed unauthorized use of Data. Licensee must perform the following:
   a) Notify the DOL by e-mail at DataServices@dol.wa.gov of such an event within 24 hours of discovery
      Identify the Data and non-conforming use of the Data.
   b) If the misuse is a criminal offense requiring notification to individuals, cooperate and facilitate with the notification of all affected individuals. At DOL's discretion, Licensee may be required to directly perform notification requirements, or if DOL elects to perform the notifications, Licensee may have to reimburse DOL for all costs associated with the notification.

WASHINGTON STATE DEPARTMENT OF LICENSING

Driver and Plate Search (DAPS) and Driver Information and Adjudication System (DIAS) Agency Access Request

Please read before completing the attached form to request access to the DAPS or DIAS (formerly IHPS) systems.

- **DAPS** – online driver and vehicle records search for use in investigations used by law enforcement, courts, prosecuting attorneys, and governmental agencies.
- **DIAS** – online system to view and electronically update driver records used by courts, prosecuting attorneys, and governmental agencies.

An executive with the authority to authorize the **Account Administrator** to contractually bind your agency for system access must sign the form. A copy of documentation that identifies the administrator as an employee of your agency (examples: employee ID, credentials, badge, etc.) is also required. Once the access request is approved, the **Account Administrator** will be required to create a License eXpress for business account and sign a click-to-agree Interagency Data Sharing Agreement for Driver and Vehicle System (DRIVES) Access ("Agreement").

Once the account is set-up, the Account Administrator will be able to add **Managers** to manage user access to the system.

It is important that you read and understand the Agreement's terms and conditions. Here is a link to the Agreement **https://www.dol.wa.gov/external/daps-dias.html** and below are some key points. Please refer to the Agreement for complete requirements:

- You will manage access of your Authorized Users in DRIVES. Their roles and responsibilities will be:
  - **Administrator** has the designated authority from your organization to click to agree on the Agreement. They will be the person responsible for administering this Agreement, and for managing all Manager and User accounts on behalf of the Licensee. The Administrator has the capability to:
    - Perform authorized functions consistent with permissions granted by DOL;
    - Request codes to add Managers and Users;
    - Revoke Manager and User access; and
    - View and search activities performed by all Authorized Users.
  - **Managers** have the capability to:
    - Perform authorized functions consistent with permissions granted by DOL;
    - Request codes to add other Managers and Users;
    - Revoke Manager and User access; and
    - View and search activities performed by all Authorized Users.
  - **Users** have the capability to:
    - Perform authorized functions consistent with permissions granted by DOL; and
    - View and search their activities.
- Each authorized user must have an individual License eXpress account.
- Access must be revoked immediately when it is no longer required for job responsibilities.
- Governmental agencies can use the data for performing their job functions, except pursuant to Executive Order 17-01, DOL data may not be used for purposes of investigating, locating, or apprehending individuals for immigration related violations.
- You must proactively ensure that information access through DAPS and/or DIAS is only used as allowed by the Agreement, and notify DOL immediately of any misuse.
- You must conduct annual assessments for Data Security, Permissible Use and Internal Control requirements of this Agreement and annually attest to DOL that you meet these requirements.

City Agreement Routing Form

The Project Administrator should complete the top section of this form, once Department Head/Designee signature has been obtained, attach the specified number of agreement originals to this form (have the contractor/supplier sign all original copies before routing) and forward the documents to the City Clerk for internal city routing. The City Clerk will route the agreement to the Risk Manager for approval of insurance and idemnification requirements, to the City Attorney for approval as to legal form and to the Mayor for signature. The City Clerk will then attest/authenticate the Mayor's signature and will forward this form and remaining agreement(s) to Project Administrator.

Project Title: Dispatch Service Level Agreement (SLA) with the Washington State Dept. of Licensing

Type of Service: for the use of Driver and Vehicle Systems (DRIVES)

Supplier/Contractor Name: Washington State Dept. of Licensing

Contract/Agreement Amount, Original: 0 Amended Amount: 0

Council Approval Date: 8/21/18 Nature of Funding: N/A

Project Administrator: Comms. Supv. Clemmons MailStop: PSPDD Phone: X2650

Anticipated Agreement Start Date: 9/4/18 Estimated Completion Date: on going

Does this contract contain the purchase of technology related items/services? ☐ YES ☒ NO

If Yes, route to: I.S. Manager (3SFN)

I.S. Signature: _____ Date: _____

Will federal funds be used to pay for all or part of contract? ☐ YES ☒ NO

If Yes, check for debarment at **www.sam.gov**
(print results and keep a copy in project file)

Department Head/
Designee Signature: Dan Handley Date: 8.28.18

Comments: Sara - Pls cross-ref AM No. 18-125

Account Numbers/
Distribution

NIGP/Commodity Code: _____

ROUTING PROCESS: (2 copies) Please return to Rena to be sent to DOL

To: City Clerk M. Date 8/29/18
(for routing and tracking)

Risk Manager Date 8/28/18
(Signature or initials)

City Attorney Date 9/4/18
(Signature or initials)

(Note: If contract exceeds Mayor's authorized signing limits, route to City Clerk (3NFN) for council approval)

Mayor Date _____
(Signature or initials)

City Clerk CK Date 9/5/18
(Signature or initials)

NOTE: The agreement becomes fully executable once the Mayor has signed it. The Project Administrator may then forward one set of originals to the Contractor/Consultant and work may begin. The City's original will be retained by the City Clerk. Once all signatures have been obtained, forward a copy of this form to Accounts Payable, with payment instructions.

Finance use ONLY Supplier Id _____ Date Received _____ Agreement # 8793