BUSINESS LICENSING SERVICES AGREEMENT

I. Parties and Contact Information

This Business Licensing Services Agreement ("Agreement") is entered into between the parties identified below:

	State of Washington Department of DOR Business Licensing Service	City of Stevenson
	("Revenue)	("Partner)
Mailing Address	PO Box 47475 Olympia, WA 98504-7475	PO Box 371 Stevenson, WA 98648-0371
Delivery Address	6500 Linderson Way, SW, Ste. 102 Tumwater, WA 98501	7121 E Loop Road Stevenson, WA 98648
Contact Person	Katie Early Phone: (360) 705-6607 E-mail: KatieE@dor.wa.gov	Leana Kinley, City Administrator (509) 427-5970 leana@ci.stevenson.wa.us

II. Purpose and Background

The purpose of this Agreement is to establish the terms under which the Business Licensing Services (BLS) program of the Department of Revenue will act as Partner's agent for the purpose of collecting, processing, and disbursing information, licenses, and fees related to Partner's licensing or other regulatory activities, hereafter referred to as Confidential Licensing Information. Partner retains all power and authority over its business licensing and other regulatory activities except as expressly delegated to Revenue under this Agreement.

Per RCW 35.090.020 (1) "a city that requires a general business license of any person that engages in business activities within that city must partner with the department (Revenue) to have such license issued, and renewed if the city requires renewal, through the business licensing service in accordance with chapter 19.02 RCW."

III. Effective Date

This Agreement is effective as of *(check **one**)* : ☐ (mm/dd/yyyy).

the date of the last signature ☒ of the parties.

IV. Services Provided by Revenue

Revenue will perform the services identified in this Section IV using best efforts in a manner determined by Revenue in good faith to be appropriate considering objectives, costs, and effectiveness.

- Distribute and process initial and renewal internet and/or paper-based applications for Partner's business licensing and/or other regulatory activities.

- Collect and process license fees and licensing information received from applicants and licensees. Disburse collected fees as directed by Partner.
- Issue Business License with Partner's license endorsement as authorized by Partner.
- Provide routine reports on Partner's business licenses as requested by Partner, which may include daily lists of new business applications and renewals, fees processed each day, weekly list of pending accounts, and lists of businesses for which fees have been transferred.
- Maintain electronic or microfilm images of all paper documents and electronic representations of electronic filings received by Revenue from applicants and provide copies or certified copies as requested.
- Maintain a database containing information received from applicants and licensees (the BLS Database).
- Provide technical assistance to establish and configure appropriate BLS Database access and secure access for Partner staff.
- Provide initial training to Partner staff in the use of the BLS Database, and ongoing training to address changes to the BLS database/access protocols or in Partner staff. Training will occur at Partner's location, over the telephone, or online, as agreed upon by the parties.
- Effect reasonable modifications in the BLS system, database, process, or forms to accommodate Partner's licensing or other regulatory requirements. Revenue will consult with Partner in evaluating alternatives and determining the most feasible and timely means of achieving Partner objectives.
- Timely notify Partner of other modifications to the BLS system, database, process, or forms, including modifications accommodating other BLS partners.

V. Partner Obligations

- Timely provide Revenue with all information requested to implement Partner's participation in the BLS program.
- Follow all requirements identified by Revenue as necessary for participation in the BLS program, including using :
    - The Business License Application and other forms and processes established by Revenue;
    - The "Business License" document for proof of licensure under Partner's licensing or regulatory program.
    - The Unified Business Identifier (UBI) number to identify licensees and license accounts in all communications with Revenue.
- Obtain and maintain at its own cost, all necessary equipment and online services required at Partner's business location(s) to support Partner's access into and use of the BLS Database. End-to-end testing will take place until such time as Revenue is satisfied.
- Ensure Partner Licensing and Information Technology staff are available to respond promptly to Revenue. Partner staff will be knowledgeable of Partner operations and/or technology and be able to assist Revenue staff with process improvements and/or troubleshooting.
- Provide timely advance notice to Revenue of potential changes to Partner business licensing requirements, fees or processes.

- Upon request by Revenue, provide statistical data associated with the BLS Partner Partnership Agreement such as Full Time Equivalent (FTE) savings, change in number of Partner licensees, and change in revenue flow.

VI. Compensation

Services identified in this Agreement are provided by Revenue at no charge with the exception of the following:

- Partner shall reimburse Revenue the costs of developing and producing ad hoc informational reports. Ad hoc reports will be created only if requested by the Partner and agreed-upon by Revenue.
- Partner shall reimburse Revenue's expenses for the implementation of changes to the BLS process, if requested by the Partner and agreed-upon by Revenue.
- All project coordination costs, including travel-related expenses, shall be absorbed by the respective parties for their own staff.

VII. Billing Procedures

Partner will provide and maintain with Revenue its current billing addresses and the personnel, if any, to whom invoices should be directed. Revenue shall submit invoices to Partner as-needed, but in no event more frequently than monthly. Partner shall pay all invoices by warrant or account transfer within thirty (30) calendar days of the invoice issue date. Upon expiration or termination of this Agreement, any claim for payment not already made shall be submitted within ninety (90) calendar days after the expiration/termination date or the end of the fiscal year, whichever is earlier.

VIII. Confidentiality and Data Sharing

The parties agree to the confidentiality and data sharing provisions set forth in Exhibit A and incorporated herein by this reference.

IX. Term and Termination

This agreement is effective until terminated. Either party may terminate this Agreement upon ninety (90) calendar days' prior written notice to the other party. This agreement may also be amended by mutual written agreement of both parties.

X. Disputes

The parties agree to participate in good faith mediation to resolve any disputes that are not otherwise resolved by agreement, prior to any action in court or by arbitration. At any time, either party may initiate formal mediation by providing written request to the other party setting forth a brief description of the dispute and a proposed mediator. If the parties cannot agree upon a mediator within fifteen (15) calendar days after receipt of the written request for mediation, the parties shall use a mediation service that selects the mediator for the parties. Each party shall be responsible for one-half of the mediation fees, if any, and its own costs and attorneys' fees.

XI. Miscellaneous

A. Governing Law and Venue**.** This Agreement shall be governed by the laws of the State of Washington. Any action arising out of this Agreement must be commenced in Thurston County, Washington.

B. Interpretation. This Agreement shall be interpreted to the extent possible in a manner consistent with all applicable laws and not strictly for or against either party.

C. No Waiver. The failure of either party to enforce any term in any one or more instance will not be construed as a waiver or otherwise affect any future right to insist upon strict performance of the term. No waiver of any term of this Agreement shall be effective unless made in writing and signed by personnel authorized to bind the party against whom enforcement is sought.

D. Assignment and Delegation. Either party may assign any right or interest, or delegate any duty or obligation, arising under this Agreement upon thirty (30) days written notice to the other party.

E. Severability. If any provision of this Agreement is held invalid by a court of competent jurisdiction, the remaining provisions of this Agreement shall be given effect to the extent consistent with applicable law and the fundamental purpose of this Agreement.

F. Survival. Terms of this Agreement which by their nature would continue beyond termination will survive termination of this Agreement for any reason, including without limitation, Sections 3 through 7 in Exhibit A.

G. No third party beneficiaries. This Agreement is for the benefit of the parties and their successors and may not be enforced by any non-party.

H. Amendments. No amendment to this Agreement is enforceable unless made in writing and signed by personnel authorized to bind the party against whom enforcement is sought.

I. Merger and integration. This Agreement contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this Agreement shall be deemed to exist or to bind any of the parties.

J. Changes in law. The provisions of this Agreement shall be deemed to change in a manner that is consistent with any changes to any directly applicable statutory authority, provided that the change is consistent with the manifest intent of this Agreement and does not conflict with any of its express provisions. Any such change to this Agreement shall be effective on the effective date of the change in authority.

IN WITNESS WHEREOF, this Agreement is executed effective as of the date specified above.

State of Washington
Department of Revenue
Business Licensing Services

_____

_____
Date

Template approved as to form

On File
Kelly Owings,
Assistant Attorney General for Washington State

Partner

_____

_____
Date

Approved as to form

_____

_____

_____
Date

EXHIBIT A

CONFIDENTIALITY AND DATA SHARING AGREEMENT

I. Purpose and Scope

The following provisions establish the terms under which the Department of Revenue ("Revenue") and Partner will share confidential data pursuant to the Business Licensing Services Agreement (the "Agreement").

II. Definitions

A. "Confidential Licensing Information" (CLI) has the same meaning as "Licensing Information" under Revised Code of Washington (RCW) 19.02.115(1)(b). CLI is classified as at least Category 3 data under Washington's Standard for Securing Information Technology Assets, Office of the Chief Information Officer (OCIO) Standard No. 141.10.
B. "Confidential Tax Information" (CTI) has the same meaning as "Return," "Tax Information," and "Taxpayer Identity" under RCW 82.32.330(b), (c), & (e). CTI is classified as at least Category 3 data under Washington's Standard for Securing Information Technology Assets, OCIO Standard No. 141.10.
C. "Confidential" refers to data classified as at least Category 3 data under Washington's Standard for Securing Information Technology Assets, OCIO Standard No. 141.10.
D. "Portable Devices" refers to small portable computing devices. Examples of portable devices include, but are not limited to handhelds/PDAs, Ultramobile PCs, flash memory devices (e.g., USB flash drives, personal media players), portable hard disks, and laptop/notebook computers.
E. "Portable Media" refers to small portable digital storage media. Examples of portable media include, but are not limited to optical media (e.g., CDs, DVDs, Blu-Rays), magnetic media (e.g., floppy disks, tape, Zip or Jaz disks), or flash media (e.g., CompactFlash, SD, MMC).
F. "Data" refers to individual pieces of information.
G. "Cloud" refers to a non-Partner data center(s) offering infrastructure, operating system platform, or software services. A more complete definition of "cloud" can be found in the National Institute of Standards (NIST) Special Publication 800-145.
H. "Encryption" refers to enciphering data with a NIST-approved algorithm or cryptographic module using a NIST-approved key length.
I. "Complex Password" or "Complex Passphrase" refers to a secret phrase, string of characters, numbers, or symbols used for authentication that is not easily guessable and meets an established industry guideline for complexity and length, such as NIST Special Publication 800-118.

III. Data Classification, Authorized Use, Access, and Disclosure

A. Data Classification: Data shared under this Agreement is considered confidential and classified as at least Category 3 data under Washington's Standard for Securing Information Technology Assets, OCIO Standard No. 141.10.
B. Permitted Uses: Business licensing information may be used for official purposes only.
C. Permitted Access: Business licensing information may be accessed only by Partner's employees and agents that have a bona fide need to access such information in carrying out their official duties.
D. Permitted Disclosure: Business licensing information received under the Agreement must not be disclosed to non-parties unless the disclosure is:

1) Ordered under any judicial or administrative proceeding; or
2) Otherwise expressly authorized by Revenue in writing.

IV. Confidentiality

Partner and Revenue each agree to keep confidential and secure from unauthorized use, access, or disclosure all confidential data received under the Agreement.

A. Ensuring Security: Partner shall establish and implement physical, electronic, and managerial policies, procedures, and safeguards to ensure that all confidential data exchanged under this Agreement is secure from unauthorized use, access, or disclosure.

B. Proof of Security. Revenue reserves the right to monitor, audit, or investigate Partner's security policies, procedures, and safeguards for confidential data. Partner agrees to provide information or proof of its security policies, procedures, and safeguards as reasonably requested by Revenue.

V. Statutory Prohibition Against Disclosure; Confidentiality Agreement

A. Criminal Sanctions. RCW 19.02.115(2) prohibits the disclosure of Confidential Licensing Information, except as expressly authorized under RCW 19.02.115(3). RCW 82.32.330(2) prohibits the disclosure of Confidential Tax Information except as expressly authorized under RCW 82.32.330(3). It is a misdemeanor for any person acquiring Confidential Licensing Information or Confidential Tax Information under this Agreement to disclose such information in violation of the disclosure limitations stated in RCW 19.02.115 and RCW 82.32.330. Partner will require employees with access to Confidential Licensing Information and/or Confidential Tax Information to sign a copy of the confidentiality agreement attached at Exhibit C.

VI. Breach of Confidentiality

In the event of any use, access, or disclosure of confidential data by Partner, or its employees or agents in material violation of the terms of this Agreement:

A. Partner shall notify Revenue in writing as soon as practicable, but no later than three working days, after determining that a violation has occurred.

B. Revenue may immediately terminate this Agreement and require the certified return or destruction of all records containing confidential data received under the Agreement.

VIII. Data Security

Confidential data provided by Revenue shall be stored in a secure physical location and on Partner-owned devices with access limited to the least number of staff needed to complete the purpose of this Agreement.

A. Partner agrees to store data only on one or more of the following media and protect the data as described:

1) Workstation hard disk drives
   a) Access to the data stored on local workstation hard disk drives will be restricted to authorized users by requiring logon to the local workstation using a unique user ID and complex password, passphrase, or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards.
   b) If the workstation is not located in a secure physical location, hard drive must be encrypted.
   c) Workstations must be maintained with current anti-malware or anti-virus software.
   d) Software and operating system security patches on workstations must be kept current.

2) Network servers
   a) Access to data stored on hard disks mounted on network servers and made available through shared folders will be restricted to authorized users through the use of access control lists, which will grant access only after the authorized user has authenticated to the network using a unique user ID and complex password, passphrase, or other authentication mechanisms that provide equal or greater security, such as biometrics or smart cards.
   b) Data on disks mounted to such servers must be located in a secure physical location.
   c) Servers must be maintained with current anti-malware or anti-virus software.
   d) Software and operating system security patches on servers must be kept current.

3) Backup tapes or backup media
   a) Partner may archive Revenue data for disaster recovery (DR) or data recovery purposes.
   b) Backup devices, tapes, or media must be kept in a secure physical location.
   c) Backup tapes and media must be encrypted.
   d) When being transported outside of a secure physical location, tapes or media must be under the physical control of Partner staff with authorization to access the data or under the physical control of a secure courier contracted by Partner for transportation purposes.

4) Cloud Storage
   a) Revenue will meet cloud and data requirements in Washington's Standard for Securing Information Technology Assets, OCIO Standard 141.10.
   b) Revenue and Partner will, at a minimum, meet the following requirements:
      i. Encrypt the data at rest and in transit.
      ii. Control access to the cloud environment with a unique user ID and complex password, passphrase, or stronger authentication method such as a physical token or biometrics.
      iii. Cloud provider data center(s) and systems must be Service Organization Control (SOC) 2 Type II certified.

5) All data provided by Revenue shall be stored on a secure environment by city staff. The City will implement these policies to ensure this security:
   a) Staff will not store or place any Revenue material on any portable devices or portable media (USB devices, CD/DVD, etc.).
   b) Staff will not email information provided by Revenue to anyone outside of City staff.
   c) Staff shall only access Revenue information on a City network computer.
   d) Staff will not save any Revenue reports or data on the hard drive of any City computer. It shall only be stored on a City network.

B. Protection of Data in Transit

Partner agrees that any retransmission of Revenue data over a network, other than the Partner's internal business network will be encrypted.

IX. Data Segregation

Revenue data must be segregated or otherwise distinguishable from non-Revenue data. This is to ensure that if the data is breached through unauthorized access it can be reported to Revenue and when the data is no longer needed by Partner, all Revenue data can be identified for return or destruction.

X. Data Breach Notification

If Partner or its agents detect a compromise or potential compromise in the data security for Revenue data such that data may have been accessed or disclosed without proper authorization, Partner shall give notice to Revenue within one (1) business day of discovering the compromise or potential compromise. Partner shall take corrective action as soon as practicable to eliminate the cause of the breach and shall be responsible for ensuring that appropriate notice is made to those individuals whose personal information may have been improperly accessed or disclosed. At a minimum, notification to Revenue will include:

A. The date and time of the event;

B. A description of the Revenue data involved in the event; and

C. Corrective actions the Partner is taking to prevent further compromise of data.

XI. Disposition of Data

A. Records furnished to the Partner in any medium remain the property of Revenue.

B. Revenue data no longer needed by the Partner must be disposed of following the data destruction procedures in this Agreement.

C. Upon the destruction of Revenue data, the partner shall complete a Certification of Data Disposition (attached to this Agreement as Exhibit B), and submit it to the Contract Manager within 15 days of the date of disposal.

XII. Data Destruction Procedures

The following are acceptable destruction methods for various types of media. At least one method defined under the various types of media must be used to destroy Revenue data for that media type.

A. Optical discs
   1) Incinerate the disc(s); or
   2) Shred the discs.

B. Magnetic tape(s)
   1) Degauss;
   2) Incinerate; or
   3) Crosscut shredding

C. Digital files on server or workstation hard drives or similar media
   1) For mechanical hard drives, use a “wipe” utility which will overwrite the data at least 3 times using either random or single character data;
   2) For solid state hard drives, use a “secure erase” utility that resets all cells to zero;
   3) Degauss sufficiently to ensure that the data cannot be reconstructed; or
   4) Physically destroy disk(s)

D. Portable media
   1) For mechanical hard drives, use a “wipe” utility which will overwrite the data at least 3times using either random or single character data;
   2) For solid state hard drives and devices, use a “secure erase” utility that resets all cells to zero;
   3) Degauss sufficiently to ensure that the data cannot be reconstructed;
   4) Physically destroying disk(s) or devices; or
   5) For SmartPhones and similar small portable devices use one of the following:
      a) If the devices are encrypted and secured with a complex password, the data is considered destroyed. Before disposal or reissuance of the device, make sure the data is encrypted and then reset the device to original or new condition; or
      b) If a Mobile Device Management (MDM) solution for the device exists, enable the remote wipe command to destroy the data.

E. Cloud Storage
   Use the cloud provider’s procedures to permanently delete the files and folders.

****end*****