STATE OF WASHINGTON

DEPARTMENT OF REVENUE

INTERAGENCY/INTERLOCAL CONTRACT BETWEEN

DEPARTMENT OF REVENUE
AND
CITY OF WEST RICHLAND

CONTRACT AMENDMENT NO. K739-1
TO
INTERAGENCY/INTERLOCAL CONTRACT NO. K739

Interagency/Interlocal Contract No. K739, by and between the Department of Revenue (REVENUE) and City of West Richland (PARTNER) is amended as follows:

BUSINESS LICESNING SERVICES AGREEMENT

I. Parties and Contact Information

Partner Contact Person revised to:

Erin Riedinger
Phone: (509) 967-7101
FAX: (509) 967-5706
E-Mail: eriedinger@westrichland.org

II. Purpose

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.

VI. Compensation

The first bullet point under this section is deleted and replaced with the following:

- The Partner shall reimburse Revenue for all fees charged by credit card processors and/or financial institutions upon any funds charged, collected, or refunded by Revenue in processing applications and/or collecting fees related to Partner's licensing or other regulatory activities. If a suitable alternative to the credit card processing can be established, eliminating the requirement of Partner reimbursement for credit card bank fees, this provision can be disregarded upon implementation of the suitable alternative without amending this Agreement. The Partner is still accountable for remaining credit card bank fees owed prior to implementation of the suitable alternative.

EXHIBIT A

1. Purpose and Scope

The following provisions establish the terms under which Revenue and Partner will share all data, including Confidential Licensing Information, pursuant to the BLS Agency Partnership Agreement (the "Agreement").

2. Definitions

"Confidential Licensing Information" has the same meaning as "Licensing Information" under RCW 19.02.115(1)(b) and includes, but is not limited to, any information included in the business license applications, renewal applications, and business licenses under the Business Licensing Service program. Confidential Licensing Information is classified as at least Category 3 data under Washington's Standard for Securing Information Technology Assets, OCIO Standard No. 141.10.

3. Confidentiality

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

A. Ensuring Security: Partner and Revenue shall each establish and implement physical, electronic, and managerial policies, procedures, and safeguards to ensure that all Confidential Licensing Information received by it 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 Licensing Information. Partner agrees to provide information or proof of its security policies, procedures, and safeguards as reasonably requested by Revenue.

4. Statutory Prohibition Against Disclosure; Secrecy Affidavit.

A. Criminal Sanctions. RCW 19.02.115 prohibits the disclosure of Confidential Licensing Information, except as expressly authorized by RCW 19.02.115. It is a misdemeanor for any person acquiring Confidential Licensing Information under this Agreement to disclose such information in violation of the disclosure limitations stated in RCW 19.02.115. Additionally, if the person is a state officer or employee, the person must forfeit such office or employment and is incapable of holding any public office or employment in Washington for a period of two years thereafter.

B. Partner will require employees with access to Confidential Licensing Information to sign a copy of the secrecy affidavit attached at Exhibit B.

5. Authorized Use, Access, and Disclosure

A. Permitted Uses: Confidential Licensing Information may be used for official purposes only.

B. Permitted Access: Confidential 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.

C. Permitted Disclosure: Confidential Licensing Information received under the Agreement must not be disclosed to non-parties unless the disclosure is:

- permitted under an express disclosure exception in RCW 19.02.115;
- ordered under any judicial or administrative proceeding; or
- otherwise expressly authorized by Revenue in writing.

D. Public Records Requests: In the event that Partner reasonably believes that it must disclose information pursuant a Public Records Request, and Partner is prohibited from disclosing such information under the terms of this Agreement, Partner must give notice to Revenue of its intention to disclose. The notice shall be provided at least 14 business days in advance of disclosure, the notice shall contain a copy of the public records request, and the notice shall reasonably identify the information that Partner believes is prohibited from disclosure under this Agreement.

STATE OF WASHINGTON

DEPARTMENT OF REVENUE

3) Partner shall instruct all individuals with access to the Confidential Licensing Information regarding the confidential nature of the information, the requirements of Use of Data and Safeguards Against Unauthorized Access and Re-Disclosure clauses of this Agreement, and the sanctions specified in federal and state laws against unauthorized disclosure of information covered by this Agreement.

ALL OTHER PROVISIONS OF THE ORIGINAL AGREEMENT WILL REMAIN IN EFFECT FOR THE CONTRACT PERIOD.

Dan Contris Chief Financial Officer Department of Revenue	12-9-2014 Date
City of West Richland	12-3-14 Date

Approved as to form:

On File Kelly Owings Assistant Attorney General	July 22, 2014 Date

6. Breach of Confidentiality

In the event of any use, access, or disclosure of Confidential Licensing Information by Partner or its employees or agents in material violation of the confidentiality 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 Licensing Information; however, Revenue shall provide Partner with an electronic record containing all information collected for Partner's licensing or other regulatory activities in an electronic medium.

7. Ownership and Retention of Records

Except as otherwise expressly provided in this Agreement, Partner may retain possession of all such records in accordance with Chapter 40.14 RCW and applicable local government retention schedules as approved by the Office of the Secretary of State.

8. Data Security

All data provided by Revenue shall be stored on a secure environment with access limited to the least number of staff needed to complete the purpose of this Agreement.

a. Protection of Data

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

1) Workstation Hard disk drives. Data stored on local workstation hard disks. Access to the data will be restricted to authorized users by requiring logon to the local workstation using a unique user ID and complex password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. If the workstation is located in an unsecured physical location the hard drive must be encrypted to protect Revenue data in the event the device is stolen.

2) Network server disks. Data stored on hard disks mounted on network servers and made available through shared folders. Access to the data 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 or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on disks mounted to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism. Backup copies for disaster recovery purposes must be encrypted if recorded to removable media.

3) Optical discs (e.g. CDs, DVDs, Blu-Rays) in local workstation optical disc drives. Data provided by Revenue on optical discs which will be used in local workstation optical disc drives and which will not be transported out of a secure area. When not in use for the Agreement purpose, such discs must be locked in a drawer, cabinet or other container to which only authorized users have the key, combination or mechanism required to access the contents of the container. Workstations which access Revenue data on optical discs must be

located in an area which is accessible only to authorized individuals, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

4) Data storage on portable devices or media.

   a) Confidential Licensing Information may be stored by Partner on portable devices or media provided the data shall be given the following protections:
      i. Encrypt the data with a key length of at least 128 bits

      ii. Control access to devices with a unique user ID and password or stronger authentication method such as a physical token or biometrics.

      iii. Manually lock devices whenever they are left unattended and set devices to lock automatically after a period of inactivity, if this feature is available. Maximum period of inactivity is 20 minutes.

      iv. Physically protect the portable device(s) and/or media by:

         - Keeping them in locked storage when not in use;

         - Using check-in/check-out procedures when they are shared; and

         - Taking frequent inventories.

   b) When being transported outside of a secure area, portable devices and media with Confidential Licensing Information must be under the physical control of Partner staff with authorization to access the data.

   c) 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.

   d) Portable media includes, but is 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).

5) Confidential Licensing Information received from Revenue will be encrypted using National Institute of Standards and Technology (NIST) approved cryptographic algorithms or modules when transmitted over the Internet, including information attached to or within email.

b. Safeguards Against Unauthorized Access and Re-disclosure

Partner shall exercise due care to protect all Confidential Licensing Information from unauthorized physical and electronic access. Partner shall establish and implement the following minimum physical, electronic and managerial safeguards for maintaining the confidentiality of information provided by either party pursuant to this Agreement:

1) Partner will store the information in an area that is safe from access by unauthorized persons when not in use.

2) Partner shall take precautions to ensure that only authorized personnel and agents are given access to on-line files containing confidential or sensitive data.

STATE OF WASHINGTON

DEPARTMENT OF REVENUE

3) Partner shall instruct all individuals with access to the Confidential Licensing Information regarding the confidential nature of the information, the requirements of Use of Data and Safeguards Against Unauthorized Access and Re-Disclosure clauses of this Agreement, and the sanctions specified in federal and state laws against unauthorized disclosure of information covered by this Agreement.

ALL OTHER PROVISIONS OF THE ORIGINAL AGREEMENT WILL REMAIN IN EFFECT FOR THE CONTRACT PERIOD.

12-9-2014

Dan Contris
Chief Financial Officer
Department of Revenue

Date

12-3-14

City of West Richland

Date

Approved as to form:

On File

Kelly Owings
Assistant Attorney General

July 22, 2014

Date