

ORIGINAL

RESOLUTION NO. 387

**A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF SHORELINE, WASHINGTON, AUTHORIZING THE ADMINISTRATIVE SERVICES DIRECTOR TO EXECUTE AN INTERLOCAL AGREEMENT BETWEEN THE STATE OF WASHINGTON DEPARTMENT OF REVENUE AND THE CITY OF SHORELINE FOR THE PURPOSE OF DATA SHARING**

WHEREAS, a Data Sharing Agreement between the Washington State Department of Revenue and the City of Shoreline is necessary to establish the terms and conditions under which the Department and the City may share confidential tax information;

**NOW, THEREFORE, THE CITY COUNCIL OF THE CITY OF SHORELINE, WASHINGTON, HEREBY RESOLVES AS FOLLOWS:**

**Section 1. Authorization to Execute Interlocal Agreement.** The Administrative Services Director is hereby authorized to execute an Interlocal Agreement between the City of Shoreline and the Washington State Department of Revenue attached hereto as Exhibit A.

**ADOPTED BY THE CITY COUNCIL ON MAY 2, 2016.**



Christopher Roberts, Mayor

**ATTEST:**

  
Jessica Simulcik Smith, City Clerk

## CITY OF SHORELINE DATA SHARING AGREEMENT FOR TAX/LICENSING INFORMATION

### I. Parties and Contact Information

	<b>State of Washington Department of Revenue</b>	<b>City of Shoreline</b>
<b>Mailing Address</b>	PO Box 47478 Olympia, WA 98504-7478	17500 Midvale Avenue N Shoreline, WA 98133
<b>Delivery Address</b>	6500 Linderson Way SW, Ste 102 Tumwater, WA 98501	Same as above
<b>Contract Manager:</b>	Sandra Yuen Phone: (360) 705-6620 FAX: (360) 705-6655 E-mail: <a href="mailto:SandraY@dor.wa.gov">SandraY@dor.wa.gov</a>	Sara Lane Administrative Services Director Phone (206) 801-2301 Email: <a href="mailto:slane@shorelinewa.gov">slane@shorelinewa.gov</a>

### II. Purpose and Authority

The purpose of this Data Sharing Agreement ("Agreement") is to establish the terms under which the Washington State Department of Revenue ("Department") and City of Shoreline ("City") may voluntarily share information of the types identified below for tax enforcement and other official purposes pursuant to Revised Code of Washington (RCW) 19.02.115(3)(j) and RCW 82.32.330(3)(h), as applicable, and [*insert statute or ordinance allowing the other party to share with Revenue*]. Nothing in this Agreement requires either party to share requested information of any kind or for any purpose.

For purposes of this Agreement, information is limited to taxpayers located within your jurisdiction or those who conduct business within your jurisdiction. The Department will, to the best of its ability, use the mailing address, physical location, or reported retail sales activity to identify the taxpayers.

### III. Attachments

This Agreement includes the following attachments, which are to be considered part of this Agreement for all purposes:

- Exhibit A Tax and License Confidentiality Affidavit
- Exhibit B Certification of Data Disposition

#### IV. Definitions

- A. **"Confidential Licensing Information"** has the same meaning as "Licensing Information" under RCW 19.02.115(1)(b). Confidential Licensing Information 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"** has the same meaning as "Returns," "Tax Information," and "Taxpayer Identity" under RCW 82.32.330(1)(b),(c), & (e). Confidential Tax Information 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. **"Agent"** means a third-party authorized representative(s) of the City or the Department that provides tax enforcement or tax regulation services to the City or the Department.
- E. **"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.
- F. **"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).
- G. **"Data"** refers to individual pieces of information.
- H. **"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.
- I. **"Encryption"** refers to enciphering data with a NIST-approved algorithm or cryptographic module using a NIST-approved key length.
- J. **"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.

#### V. 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:** Confidential Licensing Information, Confidential Tax Information and Confidential Information received under this Agreement may be used for official purposes only.
- C. **Permitted Access:** Confidential Licensing Information, Confidential Tax Information and Confidential Information may only be accessed by each party's employees that have a bona fide need to access such information in carrying out their official duties, and each party's agents that have a bona fide need to access such information for tax enforcement and tax regulation purposes.
- D. **Permitted Disclosure:** Confidential Licensing Information, Confidential Tax Information and Confidential Information received under the Agreement must not be disclosed to non-parties unless the disclosure is:
  - 1) Ordered under any judicial or administrative proceeding;
  - 2) Authorized by RCW 19.02.115 and RCW 82.32.330; or
  - 3) Otherwise expressly authorized by the Department in writing.
- E. **Public Records Requests:** In the event that City reasonably believes that it must disclose confidential or confidential tax information shared under this Agreement pursuant to a Public Records Request, and City is prohibited from disclosing such information under RCW 19.02.115 and RCW 82.32.330 and the terms of this Agreement, City must give notice to the Department of its intention to disclose. The notice shall be provided at least fourteen (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 City believes is prohibited from disclosure under this Agreement.

## VI. Information Types

- A. **"Confidential Licensing Information":** Any information identifiable to a specific licensee protected by RCW 19.02.115, including, but not limited to, information created or obtained by the Department in its administration of chapters 19.80 RCW and 59.30 RCW, and business license applications, renewal applications, and business licenses. Confidential Licensing Information protected by RCW 19.02.115 is classified as, at least, Category 3 data under Washington's OCIO Standard No. 141.10.
- B. **"Confidential Tax Information":** Any information identifiable to a specific taxpayer protected by RCW 82.32.330(1)(b), (c), & (e), including, but not limited to, a taxpayer's identity, income, assets, liabilities, tax payments, or actual or possible tax liabilities. Confidential Tax Information protected by RCW 82.32.330 is classified as, at least, Category 3 data under Washington's OCIO Standards No. 141.10.

- C. **“Confidential Information”**: Any information, except Confidential Licensing Information and Confidential Tax Information, that may legally be shared between the parties and is personal or proprietary in nature, or is exempt from public disclosure under chapter 42.56 RCW, or other state or federal law. “Confidential Information” includes, but is not limited to, Personal Information as defined in RCW 42.56.230 and RCW 42.56.590(5). Confidential Information is classified as, at least, Category 3 data under Washington’s OCIO Standards No. 141.10.

For purposes of this Agreement, Confidential Licensing Information, Confidential Tax Information and Confidential Information is limited to taxpayers located within your jurisdiction or those who conduct business within your jurisdiction. The Department will, to the best of its ability, use the mailing address, physical location, or reported retail sales activity to identify the taxpayers.

#### VII. Requesting, Receiving, and Accessing Information

The requesting party is responsible for ensuring that only persons authorized under this section are able to request, receive, or access each type of information from the other party.

- A. **Confidential Licensing Information**: Only employees who have been authorized by the receiving party may request, receive, or access Confidential Licensing Information. Authorized agents of the receiving party may receive or access Confidential Licensing Information for tax enforcement and tax regulation purposes only. The City shall ensure agents comply with RCW 19.02.115. Authorized City employees and agents must sign the Tax and License Confidentiality Affidavit, attached at Exhibit A.
- B. **Confidential Tax Information**: Only employees who have been authorized by the receiving party may request, receive, or access Confidential Tax information. Authorized agents of the receiving party may receive or access Confidential Tax Information for tax enforcement or tax regulation purposes only. The City shall ensure agents comply with RCW 82.32.330. Authorized City employees and agents must sign the Tax and License Confidentiality Affidavit, attached at Exhibit A.
- C. **Confidential Information**: Any employee or agent authorized by the receiving party may request, receive or access Confidential Information.
- D. **Confidentiality Affidavit**: The Department requires City employees and agents with access to Confidential Licensing Information and/or Confidential Tax Information to sign a copy of the Tax and License Confidentiality Affidavit, attached at Exhibit A.
- E. **Authorization**: The City will provide the Department with a regularly updated list of persons authorized to request, receive, or access Confidential Licensing Information and Confidential Tax Information. The Department will not disclose Confidential Licensing

Information or Confidential Tax Information to any person or party without a signed Tax and License Confidentiality Affidavit on file with the Department.

## VIII. Information Format

Each party will make a good faith effort to accommodate format preferences of the other party (e.g., hard copy, electronic data, CD, secure file transfer, etc.), but nothing in this Agreement requires either party to provide Information in any particular format.

## IX. Confidentiality and Security

- A. **Confidentiality:** The City and Department each agree for its employees and agents to keep confidential and secure from unauthorized use, access, or disclosure, all confidential data received under the Agreement.
- B. **Ensuring Security:** City and the Department shall each 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.
- C. **Proof of Security:** The Department reserves the right to monitor, audit, or investigate the City's security policies, procedures, and safeguards for confidential data. The City agrees to provide information or proof of its security policies, procedures, and safeguards as reasonably requested by the Department.

## X. Statutory Prohibition Against Disclosure

- 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. 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 (2) years thereafter. RCW 19.02.115(6); RCW 82.32.330(6).
- B. City will require employees and agents with access to Confidential Licensing Information and/or Confidential Tax Information to sign a copy of the Tax and Licensing Confidentiality Affidavit, attached at Exhibit A.

**XI. Breach of Confidentiality**

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

- A. City shall notify the Department in writing as soon as practicable, but no later than three (3) working days, after determining that a violation has occurred.
- B. The Department may immediately terminate this Agreement and require the certified return or destruction of all records containing confidential data received under the Agreement.

**XII. Data Breach Notification**

If City employees or its agents detect a compromise or potential compromise in the data security for Department data such that the data may have been accessed or disclosed without proper authorization, City shall give notice to the Department within one (1) business day of discovering the compromise or potential compromise. City or its agents 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 the Department will include:

- A. The date and time of the event;
- B. A description of the Department data involved in the event; and
- C. Corrective actions the City is taking to prevent further compromise of data.

**XIII. Data Security**

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

- A. City 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 disks 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 mechanism which provide equal or greater security, such as biometrics or smart cards.
    - b) If the workstation is not located in secure physical location, the 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 mechanism which 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) Optical discs (e.g., CDs, DVDs, Blu-Rays)
    - a) Data on optical discs will be used in local workstation or server optical disc drives and will not be transported out of a secure physical location.
    - b) 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.
    - c) Workstations or servers which access Department data on optical discs must be located in a secure physical location.
  - 4) Backup tapes or backup media
    - a) City may archive Department 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 if transported offsite.
    - d) When being transported outside of a secure physical location, tapes or media must be under the physical control of staff with authorization to access the data or transported by a secure courier contracted by the City for transportation purposes.
- B. Data storage on portable devices or media.
- 1) Department data stored on portable devices shall be given the following protections:
    - a) Encrypt the data.
    - b) Control access to portable devices with a unique user ID and complex password, passphrase, or stronger authentication method such as a physical token or biometrics.

- c) Control access to encrypted portable media with a unique complex password, passphrase, or stronger authentication method such as a physical token or biometrics.
  - d) Manually lock devices whenever they are left unattended or set devices to lock automatically after a period of inactivity, if this feature is available. Maximum period of inactivity is 20 minutes.
  - e) Physically protect the portable device(s) and/or media by:
    - I. Keeping them in locked storage when not in use;
    - II. Using check-in/check-out procedures when they are shared; and
    - III. Taking periodic inventories.
  - 2) When being transported outside of a secure physical location, portable devices and media with confidential Department data must be under the physical control of City staff with authorization to access the data.
  - 3) Optical disks kept in secure physical locations do not require encryption.
- C. Cloud Storage
- 1) Encrypt the data at rest and in transit.
  - 2) 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.
  - 3) Cloud provider data center(s) and systems must be Service Organization Control (SOC) 2 Type II certified.
- D. Protection of Data in Transit
- City agrees that any retransmission of Department data over a network, other than the City's internal business network, will be encrypted.

#### **XIV. Data Segregation**

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

#### **XV. Ownership and Retention of Records**

Records furnished to City in any medium remain the property of the Department. Except as otherwise expressly provided in this Agreement, City may retain possession of all such records in accordance Chapter 40.14 RCW, Preservation and Destruction of Public Records.

**XVI. Return or Destruction of Confidential Licensing Information, Confidential Tax Information and/or Confidential Information**

- A. **Return or Destruction for Violation:** The Department may, at any time, require the return or destruction of all Confidential Licensing Information, Confidential Tax Information and/or Confidential Information provided to the City during the term of this Agreement if Confidential Licensing Information, Confidential Tax Information and/or Confidential Information in the possession of the City has been disclosed, accessed, or used, or is at substantial risk of disclosure, access, or use, in violation of the terms of this Agreement.
- B. **Request for Return or Destruction.** Any request for return or destruction of Confidential Licensing information, Confidential Tax Information and Confidential Information must be in writing and provide a reasonable time for compliance. The Department may request certification in writing that all copies of the Confidential Licensing information, Confidential Tax Information and Confidential Information have been returned or destroyed.
- C. **Acceptable Destruction Methods.** The destruction of any information under this Agreement must follow the Agreement's data destruction procedures.

**XVII. Disposition of Data**

- A. Upon termination of the Agreement, the City shall dispose of the data received using the data destruction procedures in this Agreement.
- B. Upon the destruction of Department data, the City shall complete a Certification of Data Disposition, attached to this Agreement as Exhibit B, and submit it to the Department Contract Manager within fifteen (15) days of the date of disposal.

**XVIII. 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 Department 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. Server, workstation, or laptop hard drives or similar media

- 1) For mechanical hard drives, use a "wipe" utility which will overwrite the data at least three (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 three (3) times 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 destroy 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 reissue 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.

**XIX. Not a Service Agreement**

Neither party is obligated to provide services or is entitled to compensation under this Agreement.

**XX. Term and Termination**

This Agreement is effective on the date of the last signature of the parties and will remain in effect for five (5) years. The parties may enter into five (5) year extensions thereafter. Either party may terminate this Agreement at any time for any reason on fifteen (15) days written notice to the other party.

**XXI. Mediation and Arbitration**

The parties may resolve any dispute according to the specific dispute resolution provisions of this Agreement or by any other informal means. The parties agree to participate in good faith mediation to resolve any disputes relating to this Agreement that are not otherwise resolved prior to any action in court.

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 ten (10) working 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. Nothing in this Agreement shall be construed to limit the parties' choice of a mutually acceptable alternative resolution method, such as a dispute hearing, dispute resolution board, or arbitration.

**XXII. Miscellaneous Terms**

- 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. **Severability.** If any term of this Agreement shall be finally adjudicated by a court of competent jurisdiction to be unenforceable, the remainder of this Agreement will remain in full force and effect.
- D. **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, terms in Sections IX.A and IX.B (Confidentiality and Ensuring Security).
- E. **No Waiver.** The failure of either party to enforce any term in any one or more instance will not be construed as a waiver of a future right to insist upon strict performance of the term.
- F. **No Third Party Beneficiaries.** This Agreement is for the benefit of the parties and may not be enforced by any non-party.
- G. **Amendments.** No amendment to this Agreement is enforceable unless made in writing signed by personnel authorized to bind the party against whom enforcement is sought.
- H. **Notice.** Any notice required by this Agreement is effective only if provided in writing to the Contract Manager designated in Section I. Notice by email is acceptable.
- 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. **Legislative Changes.** The parties intend this Agreement to remain effective in the event of legislative change to authority cited above. The provisions of this Agreement shall be deemed to change in a manner that is consistent with any changes to cited authority,

provided that the change is consistent with the manifest intent of this Agreement and does not conflict with any express provisions. Any such change to this Agreement shall be effective on the effective date of the change in authority.

- K. **Agent Contract Terms and Conditions.** City is responsible for ensuring that all terms, conditions, and certifications in this Agreement are included in any contract with a third-party agent, in which the agent has a bona fide need to access Confidential Licensing Information, Confidential Tax Information, and/or Confidential Information for official tax enforcement or tax regulation purposes. The City shall be responsible for the acts and omissions of any of their agents.

Signed in counterparts, effective as of the date of the final signature of the parties below:

State of Washington  
Department of Revenue

City of Shoreline

\_\_\_\_\_  
(Signature) (Date)

\_\_\_\_\_  
(Signature) (Date)

\_\_\_\_\_  
(Print Name)

\_\_\_\_\_  
(Print Name)

\_\_\_\_\_  
(Title)

\_\_\_\_\_  
(Title)

TEMPLATE APPROVED AS TO FORM ONLY

On File \_\_\_\_\_  
Assistant Attorney General

EXHIBIT A



Tax and License Confidentiality Affidavit

This form must be completed and signed by every individual (including mayor, councilmember, treasurer, city manager, etc.) with access to confidential tax or licensing information.

An individual who discloses confidential information to an unauthorized person is guilty of a misdemeanor. See RCW 82.32.330(6) and 19.02.115(5).

Acknowledgement of Confidentiality

I \_\_\_\_\_ employed by \_\_\_\_\_  
(Print name)

swear or affirm that I have read and understand the requirements regarding the protection of tax and/or licensing information provided by the Department as stated in RCW 82.32.330 and 19.02.115. I further understand that this information is privileged and confidential, and therefore shall not be disclosed to any person not entitled to knowledge of such information. I understand that my use or disclosure of confidential tax and/or licensing information may be further restricted by an information-sharing agreement.

\_\_\_\_\_ (Date) \_\_\_\_\_ (Signature)

SUBSCRIBED AND SWORN TO before me this \_\_\_\_\_ day of \_\_\_\_\_,

\_\_\_\_\_  
(Signature of Notary Public)

Notary in and for the state of \_\_\_\_\_  
Residing at \_\_\_\_\_  
My commission expires \_\_\_\_\_

Authorization - Authorization is given by someone other than the person being given access to information.

I \_\_\_\_\_ of \_\_\_\_\_  
(Print name and title) (Print jurisdiction)

authorize \_\_\_\_\_ who has a business need to access the following  
(Print name and title)

from the Washington State Department of Revenue (check all that apply):

\_\_\_\_\_ Licensing Information \_\_\_\_\_ Tax Information

\_\_\_\_\_  
(Signature)

Tax and licensing information reported to the Department of Revenue (Department) is confidential and only authorized individuals with a business need may view these records. In addition, the information may only be shared with individuals in your jurisdiction who have a signed Confidentiality Affidavit on file with the Department.

**Licensing Information RCW 19.02.115**

<http://apps.leg.wa.gov/RCW/default.aspx?cite=19.02.115>

Licensing information that is collected and maintained through the Business Licensing Service (BLS) is confidential and may not be disclosed by any person unless and to the extent expressly authorized by statute, local law, or administrative rule.

Licensing information is defined under RCW 19.02.115(1)(b) and includes, without limitation, all information included in any initial and renewal business license applications and business licenses under the BLS program.

**Tax Information RCW 82.32.330**

<http://apps.leg.wa.gov/RCW/default.aspx?cite=82.32.330>

Tax information is information reported to the Department by a taxpayer, any Department actions with a taxpayer, or other data received by, recorded by, prepared by, furnished to, or collected by the Department with respect to any actions with the taxpayer. Tax information includes the taxpayer's identity, nature, source, or amount of the taxpayer's income, payments, credits, or tax payments. The following taxes are covered by this statute including but not limited to:

- Business & Occupation Tax
- Sales/Use Tax
- Lodging taxes
- Public Utility Tax
- Brokered Natural Gas (BNG)
- E-911 taxes
- Real Estate Excise Tax (REET)
- Leasehold Excise Tax

**Data Security**

Keep all data secure regardless of medium.

- ✓ Print only information you need
- ✓ Do not leave documents on printers
- ✓ Copy or download electronic data only as needed and save where only authorized persons can access
- ✓ Communication of confidential information via email, including attachments, is prohibited

**Determining Whether Information is Confidential**

Pages 3 and 5 of this form include examples demonstrating what is confidential, when information may be disclosed, and to whom it may be disclosed.

**Disclosure Penalty**

Any person acquiring knowledge of any licensing or tax information as provided under RCW 19.02.115 or 82.32.330 who discloses any such licensing or tax information to another person not entitled to knowledge of such information under the provisions of these statutes is guilty of a misdemeanor.

**Forms Submission & Questions**

Send your completed form to Patti Wilson, Local Government Liaison at [PattiW@dor.wa.gov](mailto:PattiW@dor.wa.gov). If you have questions contact by email or by calling (360) 534-1543.

**What types of tax or licensing information received from the Department are confidential?**

This table provides examples of when information your jurisdiction receives from the Department may or may not be shared with others.

#	Scenario	Confidential Information Yes or No?	Access
1.	The Mayor asks if ABC Painting is reporting sales tax to your city.	Yes, detailed information about a business's tax reporting is confidential. Even though the mayor didn't ask for actual dollar amounts, disclosing whether the business has reported or not is considered a disclosure.	If the Mayor has a business need and submitted a signed Confidentiality Affidavit to the Department, the information may be shared.
2.	A councilmember asks how much tax Jim's Plumbing has reported to your jurisdiction.	Yes, detailed information regarding a business's tax reporting is confidential.	If the councilmember has a business need and submitted a signed Confidentiality Affidavit to the Department, the information may be shared.
3.	An employee of the fire department wants to know if Joe's Automotive indicated on their business license that they would be storing flammable or toxic materials.	Yes, the information contained on the business application, including the city addendum, is confidential.	If the employee of the fire department has a business need and submitted a signed Confidentiality Affidavit to the Department, the information may be shared.
4.	The county's monthly local tax distribution amount is higher than normal due to reporting of one taxpayer. At a council meeting, the difference is discussed but no taxpayer name is disclosed.	No, talking about the distribution amounts as a whole and even stating that it is due to one taxpayer's reporting is allowed as long as the taxpayer's name and the amount the taxpayer reported is not disclosed.  The taxpayer's business activity (i.e., hotel) cannot be disclosed if there are less than three businesses with that activity in the jurisdiction.	General public, city/county staff, media

#	Scenario	Confidential Information	Access
5.	The Treasurer asks whether a business is registered and if so what is their address?	<p>No, any information contained in the on-line <u>Business Registration Lookup</u> is considered public information.                      (<a href="http://dor.wa.gov/content/doingbusiness/registermybusiness/brd/">http://dor.wa.gov/content/doingbusiness/registermybusiness/brd/</a>)</p> <p>Information contained in the Department's on-line <u>Business License Lookup</u> is also considered public information.                      (<a href="http://bls.dor.wa.gov/LicenseSearch">http://bls.dor.wa.gov/LicenseSearch</a>)</p>	General public, city/county staff, media
6.	Another jurisdiction contacts you to see if ABC Painting has reported sales tax to your jurisdiction.	Yes, the information we send one jurisdiction may not be shared with another.	<p>The Department provides each jurisdiction the information they are entitled to receive based on how the taxpayer has reported on their Combined Excise Tax Return.</p> <p>The jurisdiction requesting the information should contact the Department to investigate the taxpayer's local tax coding.</p>
7.	A reporter contacts you to confirm the amount of tax reported by a taxpayer to your jurisdiction. The reporter got the figure from the business.	Yes.	Even though the reporter got the amount from the taxpayer, any confirmation by a local jurisdiction is considered a release of confidential information.

#	Scenario	Confidential Information Yes or No?	Access
8.	A Finance Director prepares a report for a council meeting showing the sales tax distributions by NAICS code.	<p>Depends on the number of taxpayers:</p> <p><b>Yes.</b> As a policy, DOR does not disclose information when there are less than three taxpayers in a NAICS code. If there are less than three, the public or the taxpayers involved may be able to determine the income reported by the taxpayers.</p> <p><b>No.</b> If there are three or more taxpayers, there is no risk of disclosure.</p>	<p>If less than three - only the jurisdiction's employees or authorized individuals (mayor, councilperson, etc.) with a business need and a signed Confidentiality Affidavit on file may view the information.</p> <p>Three or more – general public, city/county staff, media.</p>

NOTE: A local jurisdiction may release taxpayer information if you provide the Department a Confidential Tax Information Authorization form (<http://dor.wa.gov/Docs/forms/Misc/27-0055e.pdf>) signed by the taxpayer.

To inquire about this form in an alternate format, please call 1-800-647-7706. Teletype (TTY) users may use the Washington Relay Service by calling 711.

REV 27 0056e (5/20/14)

EXHIBIT B

Certification of Data Disposition

Date of Disposition \_\_\_\_\_

\_\_\_ All copies of any data sets related to DSA No. \_\_\_\_\_ have been wiped from data storage systems.

\_\_\_ All materials and non-wiped computer media containing any data sets related to DSA No. \_\_\_\_\_ have been destroyed.

\_\_\_ All copies of any data sets related to DSA No. \_\_\_\_\_ that have not been disposed of in a manner described above, have been returned to the Department Contract Manager listed in this Contract.

The data recipient hereby certifies, by signature below, that the data disposition requirements as provided in DSA No. \_\_\_\_\_ have been fulfilled as indicated above.

\_\_\_\_\_  
(City Contract Manager Printed Name)

\_\_\_\_\_  
(City Contract Manager Signature)

\_\_\_\_\_  
(Date)

*Return original to the Department Contract Manager indicated on page one of this contract.  
Retain a copy for your records.*