APPENDIX A

ARIZONA DEPARTMENT OF REVENUE
CONFIDENTIALITY REQUIREMENTS

1. Confidential Information

1.1 Confidential Information is defined in A.R.S § 42-2001. Confidential Information may not be disclosed except as provided by statute. A.R.S. § 42-2001(B).

1.2 License information obtained from the Department of Revenue is Confidential Information and may only be disclosed as authorized by A.R.S. § 42-2003. License information obtained from other sources is not Confidential Information.

1.3 Information about a taxpayer's identity obtained from the Department of Revenue is Confidential information and may only be disclosed as authorized by A.R.S. § 42-2003. Identity information obtained from other sources is not Confidential Information.

1.4 Confidential Information includes information about a single taxpayer and also aggregated information about a group of identified or identifiable taxpayers. Aggregated information from fewer than three taxpayers in a grouping on a statewide basis or fewer than ten taxpayers in a grouping for an area that is less than state level (city or town) may be Confidential Information. Such information may not be released unless the City/Town Administrator reviews the relevant information concerning the aggregate data and makes a determination in writing that the aggregate data does not reveal information about any specific taxpayer. Such determination should take into consideration the following:

a. The proportionality of the tax information applicable to individual members of the group of taxpayers; no individual taxpayer's information should be discernable due to its relative size/taxable sales, compared to other members of the group;

b. The total aggregated tax information; the aggregate information cannot allow viewers to draw conclusions about individual taxpayers (e.g., there are 6 car dealers in the city and the total aggregate sales were $900,000 and none of them reported individual sales above the $20,000 mark, which would have qualified for the lower tax rate on large purchases)

c. Any other factor that could cause the aggregate data to be used to determine information specific to a single taxpayer.

2. Protecting Information

2.1 City/Town must identify all places, both physical and logical, where Confidential Information is received, processed and stored and create a plan to adequately secure those areas.

2.2 Confidential Information must be protected during transmission, storage, use, and destruction. City/Town must have policies and procedures to document how it protects its information systems, including Confidential Information contained therein. An example of appropriate protection standards is set forth in National Institute of Standards and Technology Special Publication 800-53. The publication may be found at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

2.3 Employees are prohibited from inspecting information unless they have a business reason for the information. Browsing information concerning friends, neighbors, family members, or people in the news is strictly prohibited.

2.4 All removable media, including paper and CDs, containing Confidential Information must be secured when not in use and after normal business hours by placing all materials in a locked drawer or cabinet. During use, Confidential Information must be protected so that it is not visible to members of the public or anyone without a business need for the information.

2.5 All individuals accessing or storing Confidential Information from an alternative work site must enter into a signed agreement that specifies how the Confidential Information will be protected while at that site. Only trusted employees shall be permitted to access Confidential Information from alternative sites. Confidential Information may not be accessed while in public places such as restaurants, lounges, or pools.

2.6 Confidential Information may not be sent outside the local area network by unencrypted email. City/Town is responsible for ensuring in-flight email communications containing Confidential Information are sent through a secure process. This may include encryption of the email message, a secure mailbox controlled by City/Town, an encrypted point-to-point tunnel between the correspondents or use of Transport Layer Security (TLS) between correspondents.

2.7 Confidential Information may not be discussed in elevators, restrooms, the cafeteria, or other public areas. Computer terminals should be placed in such a manner that prohibits public viewing of Confidential Information.

2.8 When transporting confidential materials the materials should be covered so that others cannot see the Confidential Information. When sending Confidential Information by fax a cover sheet should always be used.

2.9 Any person with unsupervised access to Confidential Information shall receive training on the confidentiality laws and requirements to protect such information before being given access to such Information and annually thereafter. They must sign certificates after the training acknowledging that they understand their responsibilities. City/Town must keep records to document this training and certification.

3. Disclosure of Information

3.1 Confidential Information may only be disclosed as permitted by A.R.S. § 42-2003.

3.2 Confidential Information is confidential by statute and, therefore, does not have to be disclosed in response to a public records request. A state agency may deny inspection of public records if the records are confidential by statute. *Berry v. State,* 145 Ariz. 12, 13 699 P.2d 387, 388 (App. 1985).

3.3 A taxpayer may designate a person to whom Confidential Information may be disclosed by completing a Department of Revenue Form 285, or such other form that contains the information included in the Form 285. City/Town may contact the Department of Revenue's Disclosure Officer if there are any questions concerning this requirement.

4. Disposal of Information

4.1 All removable media containing Confidential Information must be returned to the Department of Revenue or sanitized before disposal or release from the control of City/Town.

4.2 Paper copies of Confidential Information must be destroyed by shredding or burning the materials when no longer needed. Confidential Information may not be disposed of by placing the materials in the garbage or recycle bins. Destruction of Confidential Information may be performed by a third party vendor. City/Town must take appropriate actions to protect the Confidential Information in transit and storage before it is destroyed, such as periodic inspections of the vendor.

4.3 Computer system components and devices such as copiers and scanners that have been used to store or process Confidential Information may not be repurposed for non-tax administration uses unless the memory or hard drive of the device is sanitized to ensure under no circumstances Confidential Information can be restored or recovered.

5. Storing Data

5.1 Confidential Information may be stored on hard disks only if agency approved security access control devices (hardware/software) have been installed, are receiving regularly scheduled maintenance including upgrades, and are being used. Access controls must include password security, an audit trail, encryption, virus detection, and data overwriting capabilities.

6. Encryption Requirements and Cryptographic Module Authentication

6.1 The City/Town information system must implement mechanisms for the authentication to a cryptographic module that meets the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

6.2 Validation provides assurance that when an agency implements cryptography to protect Confidential Information, the encryption functions have been examined in detail and will operate as intended.

6.3 All electronic transmissions of Confidential Information must be encrypted using FIPS 140-2 validated cryptographic modules. A product does not meet the FIPS 140-2 requirements by simply implementing an approved security function. Only modules tested and validated to FIPS 140-2 meet the applicability requirements for cryptographic modules to protect sensitive information. NIST maintains a list of validated cryptographic modules on its website http://csrc.nist.gov/

6.4 Confidential Information is required to be protected in transit and at rest. City/Town is requested to adhere to the following guidelines to use encryption:

- Encrypt the compressed file using Advanced Encryption Standard.
- Compress files in .zip or .zipx formats.
- Use a strong 256-bit encryption key string.
- Ensure a strong password or pass phrase is generated to encrypt the file.
- Communicate the password or pass phrase with the Department of Revenue through a separate email or via a telephone call to your DOR contact person. Do not provide the password or passphrase in the same email containing the encrypted attachment.

6.5 Refer to your specific file compression software user guide for instructions on how to compress and encrypt files. Known compatible products with DOR include but are not limited to WinZip and Secure Zip.

6.6 Please remember, while the attachment is encrypted, the content of the email message will not be encrypted, so it is important that any sensitive information be contained in the attachment (encrypted document).

7. Wireless Access (if accessing State Confidential Information from a wireless network)

7.1 City/Town must:

- Establish restrictions, configuration/connection requirements, and implementation guidance for wireless access.
- Authorize wireless access to the information system prior to allowing such connections.
- Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.

8. Interconnection Security Agreement

8.1 Trusted Behaviors. The City/Town system and users are expected to protect ADOR's data in accordance with applicable state and federal laws.

8.2 Data Flows. The City/Town is responsible for creating architectural diagrams of any systems connecting to ADOR systems and depicting the flow of State Confidential Information.

8.3 Audit Trail Responsibilities. City/Town is responsible for auditing application processes and user activities involving any information interconnection. Activities that will be recorded include event type, date and time of event, user identification, workstation identification, success or failure of access attempts, and security actions taken by system administrators or security officers. Audits, and/or security actions taken by system administrators or security officers will be recorded and available for review by ADOR.

8.4 Incident Reporting. City/Town is required to notify ADOR in the event of data loss, breach, or security concern regarding ADOR's Confidential Information by reporting the incident to the ADOR Information Security Team by phone at (602) 716-6166 or email at InfoSec@azdor.gov.

8.5 DOR may send employees or auditors to inspect any of City/Town information systems and/or facilities used to process, store or transmit any ADOR data at any time to ensure that ADOR information is adequately protected.

APPENDIX B

From the effective date of this Agreement until the new functionalities set forth below are implemented, the Department of Revenue will provide the following reports:

City Payment Journal Detail;
City Payment Journal Summary;
New License Report

Within 30 days after the first month's implementation of the JT2, the Department of Revenue will provide a new License Report and License Update Report containing at least the following fields:

NEW LICENSE REPORT AND LICENSE UPDATE REPORT

Fields displayed:

- Region Code
- Run Date
- Report Start Date
- Report End Date
- Update Date
- ID Type
- ID
- Account ID
- Entity Name
- Ownership Type
- License ID
- OTO/Applied For indicator
- Bankruptcy Indicator
- Filing Frequency
- Issue Date
- Account Start Date
- Business Start Date
- Arizona Start Date
- Doc Loc Nbr
- Accounting Method
- Close Date
- Close Code
- Business Description
- NAICS1
- NAICS2
- NAICS3
- NAICS4
- Mailing Street1
- Mailing Street2

- Mailing Street3
- Mailing City
- Mailing State
- Mailing ZIP
- Mailing Country
- Mailing Phone Number
- Mailing Address Add date
- Mailing Address End Date
- Audit Street1
- Audit Street 2
- Audit Street 3
- Audit City
- Audit State
- Audit Zip
- Audit Country
- Audit Phone Number
- Audit Address Add Date
- Audit Address End Date
- Location Code
- Business Codes
- Location Name (DBA)
- Number of Units
- Location Street 1
- Location Street 2
- Location Street 3
- Location City
- Location State
- Location Zip
- Location Country
- Location Phone Number
- Location Start Date
- Location End Date
- Primary Location Street 1
- Primary Location Street 2
- Primary Location Street 3
- Primary Location City
- Primary Location State
- Primary Location Zip Code
- Primary Location Country
- Primary Location Phone Number
- Primary Location Start Date
- Primary Location End Date
- Owner Name
- Owner Title
- Owner Name 2
- Owner Title 2

- Owner Name 3
- Owner Title 3

Within 30 days of the implementation of the TPT2, the Department of Revenue will provide the following reports with at least the fields indicated below:

CITY PAYMENT JOURNAL

- Run Date
- Report Start Date
- Report End Date
- GL Accounting Period
- Period End Date
- Payment received date
- Return received date
- Payment process date
- Return process date
- Filing Frequency
- License ID
- Entity Name
- Location Code
- Location Name (DBA)
- Location Street 1
- Location Street 2
- Location Street 3
- Location City
- Location State
- Location Zip
- Location Country
- NAICS
- Business Code
- Doc Loc Nbr
- Pmt Loc Nbr
- Gross Receipts
- Total Deductions
- Tax or Fee Collected
- P & I Collected
- Audit Collections
- Tran Type
- Tran Subtype
- Rev Type

CITY PAYMENT JOURNAL SUMMARY

- Region Code
- Run Date
- Report Start Date
- Report End Date
- GL Accounting Period

- Business Code
- Number of Accounts
- Collections

Within 30 days after the first month's implementation of the TPT2, the following reports with at least the fields indicated below:

NO MONEY REPORT

- Region Code
- GL Accounting Period
- Period End Date
- Payment received date
- Return received date
- Payment process date
- Return process date
- Filing Frequency
- License ID
- Entity Name
- Location Code
- Location Name (DBA)
- Location Street 1
- Location Street 2
- Location Street 3
- Location City
- Location State
- Location Zip
- Location Country
- NAICS
- Business Code
- Doc Loc Nbr
- Pmt Loc Nbr
- Gross Receipts
- Total Deductions
- Tax or Fee Collected
- P & I Collected
- Audit Collections
- Tran Type
- Tran Subtype

DEDUCTION REPORT

- Region Code
- Run Date
- Report Start Date
- Report End Date
- GL Accounting Period
- Period End Date

- License ID
- Entity Name
- Location Code
- Location Name (DBA)
- Business Code
- Doc Loc Nbr
- Deduction Code
- Deduction Amount
- Tran Type
- Tran Subtype
- Rev Type

Within 30 days after taxes (subject to fund distributions) are collected, the Department of Revenue will provide the following report with at least the fields indicated below:

FUND DISTRIBUTION REPORT

- Region Code
- Run Date
- Report Start Date
- Report End Date
- GL Accounting Period
- Period End Date
- Payment Received Date
- Return Received Date
- Payment Processed Date
- Return Processed Date
- License ID
- Entity Name
- Location Code
- Location Name (DBA)
- Business Code
- Doc Loc Nbr
- Fund Allocation Code
- Amount Distributed

FUND DISTRIBUTION SUMMARY REPORT

- Region Code
- Run Date
- Report Start Date
- Report End Date
- GL Accounting Period
- Fund Allocation Code
- Amount Distributed