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. The acceptable encryption algorithms are set forth in the standards attached as Exhibit 1, which may be updated to accommodate changed technology.

2.7 Confidential Information may not be discussed in elevators, restrooms, the cafeteria, or other public areas. 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.

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 Confidential Information may 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.

EXHIBIT 1

ENCRYPTION STANDARDS

1.0 Acceptable Encryption Algorithms – The following encryption algorithms are considered acceptable for use in information systems to protect the transmission or storage of Confidential Information and system access.

1.1.1 Acceptable Security Strength – the security strength of an encryption algorithm is a projection of the time frame during which the algorithm and the key length can be expected to provide adequate security. The security strength of encryption algorithms is measured in bits, a measure of the difficulty of discovering the key.

a. The current minimum key strength for Confidential Information is 112 bits.

1.1.2 Symmetric Encryption Algorithms – The following symmetric encryption algorithms are considered acceptable for use.

Algorithm	Reference	Acceptable Key Strengths
Advanced Encryption Standard (AES)	FIPS 197	128, 192 or 256 bits
Triple Data Encryption Algorithm (TDEA) (three key 3DES)	SP 800-67	168 bits

1.1.3 Key Agreement Schemes – The following key agreement schemes are considered acceptable for use

Key Agreement Scheme	Reference	Acceptable Key Strengths Finite Fields	 Elliptical Curves
Diffie-Hellman (DH) or MOV	SP 800-56A SP 800-135	P = 2048 Q = 224 or 256	N: 224-255 and H=14 N: 256-383 and H=16 N: 384-511 and H=24 N: 512+ and H=32
RSA – based	SP 800-131A	N = 2048	

1.1.4 Hash Functions – The following hash functions are considered acceptable for use

Digital Signature Generation	Digital Signature Verification	Non-digital signature generation applications
SHA-224 SHA-256 SHA-384	SHA-224 SHA-256 SHA-384	SHA-1 SHA-224 SHA-256

SHA-512	SHA-512	SHA-384 SHA-512

1.1.5 Digital Signature Algorithms – The following digital signature algorithms are considered acceptable for use.

Digital Signature Algorithm	FIPS Publication	Digital Signature Generation Settings	Digital Signature Verification Settings	Relative Strengths
Digital Signature Standard (DSA)	FIPS 186-4	p>= 2048 q = 224	p>= 2048 q = 224	>= 112 bits
RSA Digital Signature	FIPS 186-4	2048	2048	>= 112 bits
ECDSA	FIPS 186-4	224	224	>= 112 bits

1.1.6 Message Signature Algorithms – The following digital signature algorithms are considered acceptable for use.

Hash Algorithms	Hash Generation	Hash Verification
HMAC	>= 112 bits	>= 112 bits
CMAC	AES, 3DES	AES, 3DES
CCM and GCM/GMAC	AES	AES