ARIZONA

UNIFORM REAL PROPERTY ELECTRONIC

RECORDING ACT

REPORT FROM THE ARIZONA ELECTRONIC RECORDING COMMISSION

Pursuant to A.R.S. §§ 11-487 to *11-487.06 (This section is repealed by Laws 2005, Ch. 109, § 2, effective January 1, 2008.)*

Effective November 1, 2007

TABLE OF CONTENTS

Arizona Electronic Recording Commission members:

Hon. Helen Purcell, Commission Chair	Maricopa County Recorder
Hon. Laura Dean-Lytle	Pinal County Recorder
H. Ross Jameson, CMC	Premier Financial Services, Inc.
John T. Lotardo, Esq.	Stewart Title and Trust of Phoenix, Inc.
Scott Malm, Esq.	Gust Rosenfeld, PLC
Hon. F. Ann Rodriguez	Pima County Recorder
Hon. Ana Wayman-Trujillo	Yavapai County Recorder

The Arizona Electronic Recording Commission is responsible for the adoption of standards to implement the Arizona Uniform Real Property Electronic Recording Act (Arizona URPERA), A.R.S. §§ 11-487 (Laws 2005, Ch. 109, effective Jan. 1, 2006) to *11-487.06 (This section is repealed by Laws 2005, Ch. 109, § 2, effective January 1, 2008.)*

Arizona Electronic Recording Commission
Arizona Uniform Real Property Electronic Recording Act

Section I: Introduction

The Arizona legislature established the Arizona Electronic Recording Commission (AERC) to adopt standards to implement the Uniform Real Property Electronic Recording Act (URPERA). Passed during the 2005 legislative session, the Arizona URPERA authorizes county Recorders to accept electronic documents for recording, provided that they do so in compliance with standards established by the AERC. The AERC is composed of seven members representing a range of stakeholders in the real property recording process:

1. Four members who are county recorders in this state.
2. One member who represents an association of title companies.
3. One member who represents an association of mortgage bankers.
4. One member who represents real property lawyers.

The AERC, in accordance with the provisions of its authorizing legislation, used the electronic recording standards issued by the Property Records Industry Association (PRIA) as the foundation for Arizona standards, expanding upon or clarifying the PRIA standards when necessary. AERC standards address the following issues:

Data standards
Security (transactional and organizational)
Electronic signatures
Notary acknowledgment
File formats for electronic recording
Records retention and preservation
Payment of fees

The Arizona Uniform Real Property Electronic Recording Act will be updated periodically in response to changes in the technological environment.

For a glossary of terms referenced in this document, see Appendix A. For acronyms referenced in this document, see Appendix B. For an explanation of electronic recording models, see Appendix C. For applicable Arizona statutes pertaining to electronic recording, see Appendix D.

Section II: Arizona Uniform Real Property Electronic Recording Act

1) Data Standards.

The AERC adopts the PRIA standards on electronic document formatting and document data elds.

Comments

PRIA data and document standards are the preferred standard for use by industry participants of electronic document recording. See Appendix for a list of the PRIA standards and supporting documents.

It is further recommended that eRecording be o ered and conducted at all three models of submission. See Appendix C for an explanation of e-recording models from the PRIA Implementation Guide.

2) Security.

Participants of electronic recording shall develop security standards and policies based on industry accepted security practices and protocols.

Comments

Transactional Security: All electronic documents must be secured in such a way that both the transmitting and receiving parties are assured of each other's identity, and that no unauthorized party can view or alter the electronic document during transmission, processing, and delivery. If the electronic document has been subject to those security measures identi ed in Chapter 6 of the *PRIA eRecording XML Implementation Guide For Version 2.4.1, Revision 2, Updated 03/05/2007* throughout the entire electronic document process of execution through recording, then the security obligations under these standards have been satis ed.

Organizational Security: Each Recorder's o ce, which elects to accept electronic documents for recordation pursuant to A.R.S. §§ 11-487 to *11-487.06 (This section is repealed by Laws 2005, Ch. 109, § 2, effective January 1, 2008)*, shall implement reasonable measures such that each electronic document accepted for recordation is protected from alteration and unauthorized access.

3) Electronic Signatures.

While Uniform Electronic Transactions Act (UETA), 15 U.S.C.A. §§ 7001 to 7031 (Information can be found at: http://www.law.upenn.edu/bll/archives/ulc/fnact99/1990s/ueta99.htm) and URPERA allow many types of electronic signatures, Recorders are only required to accept electronic signatures that they have the technology to support.

4) Notary Acknowledgement.

Transactions filed pursuant to A.R.S. §§ 11-487 to *11-487.06 (This section is repealed by Laws 2005, Ch. 109, § 2, effective January 1, 2008)* must comply with A.R.S. §§ 41-311 to 41-370 as amended from time to time.

5) Document Formats for Electronic Recording.

The AERC recommends that electronic recordings be converted to (if necessary) and preserved as TIFF or PDF files along with their associated metadata. Model 3 submissions should be converted to TIFF or PDF until the viability of preserving these eRecordings in their native format (i.e. XML, XHTML) has been demonstrated.

Comments

Recommended Preservation File Formats (See Appendix F):

TIFF: The Tagged Image File Format (TIFF) is widely adopted within the property recording industry and by recorders who have imaging systems. TIFF is a non-proprietary format that is recommended for storing scanned images.

PDF: Portable Document Format (PDF) is another commonly used file format in the property recording industry. PDF files capture the appearance of the original document, can store both text and images, are difficult to modify, and can be rendered with free, cross-platform viewer software. PDF is based on publicly available specifications, and as of January 2007 Adobe, the creator of the format, is releasing the 1.7 version of the format to become an international standard through the International Standards Organization (ISO).

XML: Extensible Markup Language (XML) is the recommended file format for long-term preservation of any metadata.

Metadata: Metadata is commonly described as "data about data." Metadata is used to locate and manage information resources by classifying those resources and by capturing information not inherent in the resource. In the eRecording context, metadata may be generated automatically or created manually and it may be internal or external to the digital object itself. Regardless of how it is created or stored, maintaining accurate and reliable metadata is essential to the long-term preservation of eRecordings.

Microfilm: The archival process for electronic records will require consistent and complex management in order to maintain authenticity and integrity. Digital preservation requires a well-developed plan and implementation with specific policies and procedures. Electronic records are subject to the same threats of destruction as other mediums such as natural or human-made disasters. There are the added challenges of hardware and software obsolescence, media longevity and migration, infrastructure failures and accidental damage from improper handling.

The majority of records in the custody of the Recorders must be preserved permanently. The durability of electronic records has not been proven to be as enduring as microfilm. In order to secure and preserve information created and stored electronically, security microfilm is recommended. Microfilm is an analog technology that allows documents to be read with magnification and a light source. If necessary, microfilm can be converted into a digital format. Producing microfilm that is created within the guidelines of the American National Standards Institute (ANSI) and properly stored and handled should provide secure records for hundreds of years.

6) Records Retention and Preservation.

Recorders must retain all records in their custody in accordance with requirements detailed in each County Recorder's record retention schedule, approved by the Arizona State Library, Archives and Public Records.

Comments

See Appendix F for guidance on the long-term preservation of electronic recordings.

7) Payment of Recording Fees.

Electronic payment of recording fees shall be collected by public agencies as prescribed by state and local statutes and in accordance with accepted industry standards without incurring unreasonable electronic processing fees.

Comments

Payments are a prerequisite to all methods of recording. Whether or not a payment is attached or an authorization of payment is included in a recording submission, the submission must incorporate some methodology for payment of fees associated with a particular document or set of documents.

Typical payment options include: ACH (Automated Clearing House), internal escrow accounts, credit and debit cards, and journal vouchers. The majority of jurisdictions interviewed currently engaged in electronic recording collect payment through ACH or by internal escrow accounts.

Fees are to be collected according to statute and in a manner consistent with the promotion of electronic recording, and in accordance with accepted industry standards. Each county recorder may collect electronic recording fees in a manner compatible with its internal software and county financial practices.

Section III: Appendices

APPENDICES

A) Glossary of Terms

B) Acronyms Used In This Document

C) Electronic Recording Models Explained

D) Related Statutes and Regulations

E) PRIA Standards and Guidelines

F) Records Retention and Preservation Statutes

G) Model Memorandum of Understanding

H) Frequently Asked Questions

Appendix A
Glossary of Terms

Asymmetric encryption: A method that uses two keys – a public key and a private key. Together, the keys constitute a key pair. Though the keys are mathematically related, it is not possible to deduce one from the other. The public key is published in a public repository and can be freely distributed. The private key remains secret, known only to the key holder.

Authentication: The act of tying an action or result to the person claiming to have performed the action. Authentication generally requires a password or encryption key to perform, and the process will fail if the password or key is incorrect.

Digital signature: A type of electronic signature consisting of a transformation of an electronic message using an asymmetric crypto system such that a person having the initial message and the signer's public key can accurately determine whether:

(1) the transformation was created using the private key that corresponds to the signer's public key; and

(2) the initial message has not been altered since the transformation was made.

Digitized signature: A representation of a person's handwritten signature, existing as a computerized image file. Digitized signatures are just one of several types of electronic signatures, and have no relation to digital signatures.

Document type definition (DTD): A document created using the Standard Generalized Markup Language (SGML) that defines a unique markup language (such as XHTML or XML). A DTD includes a list of tags, attributes, and rules of usage.

Electronic commerce: Also known as e-commerce, it refers to trade that occurs electronically, usually over the Internet. Electronic commerce often involves buying, selling, and sharing information, extending both new and traditional services to customers via electronic means. E-commerce allows business to take advantage of email, the Web, and other online innovations to improve the business process and offer consumers more ways to access products, faster information transfer and ultimately decreasing costs.

Electronic document: A document that is received by the Recorders in an electronic form.

Electronic record: A record created, generated, sent, communicated, received or stored by electronic means.

Electronic notary: A notary public who has registered with the Secretary of State and who provides electronic notarial acts using a digital certificate authorized by the Secretary of State. (A.R.S. §§ 41-351 to 41-370)

Electronic signature: An electronic sound, symbol or process attached to or logically associated with a document and executed or adopted by a person with the intent to sign the document. (See also A.R.S. § 11-487.01(4) and A.A.C. R2-12-501)

Encrypt: To apply an encryption key to a message in order to make it unreadable in an effort to prevent unintended use of the information.

Extensible Markup Language (XML): A computer language used to create markup languages. XML allows developers to specify a document type definition (DTD) or schema in order to devise new markup languages for general or specific uses.

Hash function: A mathematical algorithm that takes an electronic document and creates a document fingerprint. The document fingerprint is much smaller than the original document, and does not allow the reconstitution of the original document from the fingerprint. A slightly different document, processed through the same hash function, would produce very different document fingerprint. A hash function helps to secure data by providing a way to ensure that data is not tampered with.

Key pair: A set of keys, including a private key and a public key, used in asymmetric cryptography. Sometimes a key pair will be reserved for specific uses, such as creating digital signatures (signing pair) or encrypting secret information (encryption pair).

Metadata: Commonly described as "data about data." Metadata is used to locate and manage information resources by classifying those resources and by capturing information not inherent in the resource.

Nonrepudiation: Effectively implementing a process in such a way that the creator of a digital signature cannot deny having created it. Nonrepudiation involves supplying enough evidence about the identity of the signer and the integrity of a message so that the origin, submission, delivery, and integrity of the message cannot be denied. Protection of a user's private key is also a critical factor in ensuring nonrepudiation. The entire Public Key Infrastructure (PKI) industry exists to create and ensure the trust necessary for nonrepudiation.

Notary public: "Notary public" and "notary" mean any person appointed by the Secretary of State to perform notarial acts.

Portable Document Format (PDF): A file format created by Adobe Systems, Inc. that uses the PostScript printer description language to create documents. PDF files capture the appearance of the original document, can store both text and images, are difficult to modify, and can be rendered with free, cross-platform viewer software.

Portal: In eRecording terms, an electronic location where submitters can send their documents for further processing and delivery. A fully featured portal will incorporate specific index rules and information from other tables that assure conformity with the receiving County's backend recording system. A portal should be capable of receiving various document types from various submitting parties and be able to deliver them to virtually any county regardless of their back end recording system or physical location.

Private Key: A large, randomly generated prime number used in asymmetric encryption. The private key is used to encrypt a document fingerprint (the result of processing an electronic document through a hash function) to create a digital signature. A private key is generated by its holder at the same time a related public key is created. While the public half of a key pair is made available to anyone who wants it, the private key is only known by its owner, who must keep it absolutely secret to maintain its integrity.

Proprietary: Indicates that software or other employed technology is owned or controlled exclusively by the vendor. These solutions are not transferable to other systems and must be used only on the vendor's systems.

Public Key: A large, randomly generated prime number that is used to decrypt an electronic document that has been encrypted with a private key. A public key is generated by its holder at the same time a related private key is created. Within the Public Key Infrastructure (PKI), public keys are used to verify digital signatures. Public keys are contained in digital certificates, published and otherwise distributed by the issuing certificate authority (CA).

Public Key Infrastructure (PKI): The framework of different entities working together to create trust in electronic transactions. The PKI industry facilitates signed transactions by using asymmetric cryptography to ensure security and verifiable authenticity. The PKI includes all parties, policies, agreements and technologies to a transaction. This sophisticated infrastructure allows all concerned parties to trust electronic transactions created within the standards set by the PKI industry.

Schema: A method for specifying the structure and content of specific types of electronic documents which use XML.

Secure Socket Layer (SSL): A security technology that uses both asymmetric and symmetric cryptography to protect data transmitted over the Internet.

Signature Authentication: The process by which a digital signature is used to confirm a signer's identity and a document's validity.

Signed Digital Document: An electronic document that includes an embedded digital signature. The digital signature contains an encrypted document fingerprint, which allows anyone receiving the document to verify its validity using the process of signature authentication.

SMART Doc™: A SMART Doc™ is a technical framework for representing documents in an electronic format. This format links data, the visual representation of the form, and signature. The visual representation of the documents can utilize a variety of technologies such as XHTML, PDF, and TIFF. Previously SMART docs™ were called eMortgage documents. In order to better describe the actual capabilities of the technology, the word "eMortgage" was replaced by the acronym "SMART" which represents: Securable, Manageable, Archivable, Retrievable, and Transferable.

Submitting Party: The entity that originates an electronic document. This is usually a bank, title company, attorney or anyone that inputs data into a specific template and/or associates an image and wishes to send the documentation for electronic recordation at the County.

Tagged information file format (TIFF): An image file format commonly used for photos, scanned documents, or other graphics. TIFF images are graphics that are made up of individual dots or pixels. Files in the TIFF format are distinguished by a .tif filename extension.

Third party vendor: Entity that may act as a middle man or liaison to an electronic transaction. The vendor will usually have some added value to the transaction such as verifying accuracy and completeness of index entries, authentication of the submitting party, or any other County specific requirement.

Uniform Electronic Transactions Act (UETA): A body of recommended legislation drafted in 1999 by the National Conference of Commissioners on Uniform State Laws (NCCUSL) for adoption by state legislatures. UETA allows electronic documents and digital signatures to stand as equals with their paper counterparts. Arizona adopted a modified version of UETA (see A.R.S. §§ 44-7001 to 44-7051).

Uniform Real Property Electronic Recording Act (URPERA): A body of recommended legislation drafted in 2004 by the National Conference of Commissioners on Uniform State Laws (NCCUSL) for adoption by state legislatures. URPERA authorizes Recorders to accept electronic documents for recording in accordance with established standards. Arizona adopted a modified version of URPERA (see A.R.S. §§ 11-487 to *11-487.06 (This section is repealed by Laws 2005, Ch. 109, § 2, effective January 1, 2008.)*).

Wet signature: An original representation of a person's name applied to a document. Wet signatures are often highly stylized, sometimes bearing little resemblance to the name they are supposed to represent.

XML: See Extensible Markup Language.

XML Schema: See Schema.

Appendix B
Acronyms Used In This Document

AERC	Arizona Electronic Recording Commission
AETA	Arizona Electronic Transactions Act
ACH	Automated Clearing House
ANSI	American National Standards Institute
DTD	Document Type Definition (see Glossary)
E-SIGN	Electronic Signatures in Global & National Commerce
FTP	File Transfer Protocol
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ISO	International Standards Organization
MISMO	Mortgage Industry Standards Maintenance Organization
MOU	Memorandum of Understanding
NCCUSL	National Conference of Commissioners on Uniform State Laws
OAIS	Open Archival Information Systems
PDF	Portable Document Format
PKI	Public Key Infrastructure (see Glossary)
PRIA	Property Records Industry Association

RESVQ SSL	Secure Socket Layer (see Glossary)
TIFF	Tagged Information File Format (see Glossary)
UETA	Uniform Electronic Transaction Act
URPERA	Uniform Real Property Electronic Recording Act
VPN	Virtual Private Network
XHTML	Extensible Hyper Text Markup Language
XML	Extensible Markup Language (see Glossary)

Appendix C
Electronic Recording Models Explained

From the PRIA I-Guide©

2.3 eRecording Models

Electronic recordings, whether as pilot projects or live production initiatives, have occurred in twenty states. From these efforts, three distinct models have emerged. The models are referred to as Models 1, 2 and 3. Each has distinctive characteristics. Each also brings certain benefits to the submitters.

Over time the improvements in delivery methods and document formats have improved the processes as well. From scanned paper documents, to electronically-signed images of the documents wrapped with XML data and securely signed, to completely electronic, XML-integrated documents using electronic and digital signatures, these models bring continuing benefits to participating recorders and document submitters. Ongoing progress with increasing value from added benefits are expected as mortgage, legal and recording industry standards are implemented.

2.3.1 Model 1

Description

This model is an extension of the paper-based closing or payoff processes. Documents are prepared and printed. The parties sign and notarize the paper documents with ink signatures. When complete, the signed and notarized paper documents are scanned and electronically sent to the recorder. Transmission is done by the submitting parties logging on to the recorder's computer system over a secure network after first identifying, or authenticating, themselves to the recorder's computer. The recorder makes the same determination of record- ability as with paper documents, visually inspecting them for such things as signatures and acknowledgments as well as determining the recording fees. Fees are usually paid from an escrow account the submitter maintains with the recorder.

Once the recorder accepts the documents for recording the scanned image is "burned" with the recording information, including recording date and time as well as the unique recording reference number, such as book and page number or instrument number. Indexing is performed by the indexing staff of the recorder's office, as are paper documents. A copy of the recorded images is returned to the submitter. Usually a recording receipt, together with the recording endorsement data, is returned to the submitter, who uses the data to create and print a label with the recording endorsement information. The label is affixed to the paper document, which is then processed as usual by the submitter. In other jurisdictions, the paper document is fed through a printer and the recording endorsement information is printed on document (usually on the upper, right-hand corner of the first page).

In jurisdictions that use Model 1, such as Orange County, California, and Maricopa County, Arizona, the average elapsed time for the process is usually under an hour from the time the recorder receives the image until the receipt and data are returned to the submitter.

2.3.2 Model 2

Description

Model 2 recordings may be paper or electronic based. A document image whether from a scanned paper document signed and notarized by 'wet ink' signatures or from an electronic document electronically signed and notarized, is wrapped in an XML wrapper containing the data necessary for processing, indexing and returning the document. In the case of a scanned paper document, Model 2 further extends Model 1 by adding data that improves the process, specifically the indexing process in the recorder's office. In the case of an electronic document, it begins to improve the process for the settlement agent, lender or loan servicer submitting the document.

The model may support one or more of a number of graphics formats. Uncompressed TIFF (Tagged Image File Format) images are commonly used, because this format preserves the image in the most accurate and legible form.

The recordable documents are generally delivered to the county recorder's site by whatever means the parties agree, including hypertext transport protocol secure (HTTPS), web services, file transport protocol (FTP) and even email. Most counties require some authentication of the submitter, typically based on an account and personal identification number (PIN), although some use digital signatures and certificates in lieu of, or in addition to, the former. The documents are stored in a secure area on the recorder's web site until the recorder's system retrieves them.

Once imported into the recorder's system, the recorder's legacy system handles the recording functions. In this case the system imports the data from an XML wrapper, including index data. The recording process is partially automated, but the image must be visually inspected to determine that it meets recording requirements as well as possibly to validate against the data in the XML wrapper. The indexing data in the embedded image is not linked to the index data in the XML, so the recorder has no automated means to verify that it is the same.

If a document meets the requirements, it is recorded. The recording information is "burned" onto the image and returned to the submitter by means agreed upon by the parties. In some jurisdictions that use Model 2, the electronic recorded document is embedded into an XML wrapper with the recording information added so that the submitter can use the data in its internal processes.

The average elapsed time from receipt to returning the recorded electronic documents is about five minutes for Broward County, Florida. That compares to about five days for similar closing documents delivered by settlement agents. Average turn around for mail-in documents is about seven days.

2.3.3 Model 3

Description

In a number of counties electronic reconveyances of deeds of trust and satisfactions of mortgages are prepared by loan servicers and electronically submitted. Under Model 3, these real estate documents are generated on a vendor's document preparation system in XHTML

(extensible hypertext mark-up language) format. The document preparation person logs on to the system and enters the information necessary to complete the generation of the document. Once the document has been generated, the person signs it if she has the authority, or notifies the person with signing authority to sign. Secure access is required for all parties that must sign the document because signing is done by digital signature.

Once the documents are electronically signed and notarized, they are released for recording. The document preparation system compares each document against recording rules to ensure its recordability, and then calculates recording fees. Documents may be submitted in batches. Submission is by secure hypertext transport protocol (HTTPS) through the vendor's recording server to the recorder's office.

Documents received at the recorder's system are re-checked against the rules to determine whether or not they may be recorded. If not, they are returned to the submitter. Otherwise they are accepted for recording and the data for recording is extracted from the documents and passed to the legacy recording system. The endorsement data is received from the legacy system and entered onto the respective documents in XML format. If required, the XHTML is transformed to TIFF images for the recorder's archives and the XHTML documents with the recording endorsements are returned to the submitter.

Fee payment information is passed to the legacy system after the rules determine that the recording fees are correct. The recorder collects the fees from escrow accounts maintained by the respective submitters, or by Automated Clearing House (ACH) payment processing.

The average turnaround time is approximately 30 seconds from the time the recorder receives the document until the recorded document is returned. This time includes the entire process, from quality control verification to indexing, when run in an "unattended" or "lightsout" mode.

Characteristics of different eRecording Models

	Model 1	Model 2	Model 3
Document Type	Paper closings are scanned as TIFF images; no data is associated with the TIFF image. The recorder views the TIFF images to process the submission.	Electronic or paper closings are supported. The electronic document, whether image or other format is embedded in theXML "wrapper." Of index data and other information. The recorder processes the submission primarily from the data "wrapper". The recorder also has the option to view the document to validate data or image quality, or review the document to meet other requirements.	A single electronic file with both the signed document and indexing data is submitted and able to be processed by the recorder. Currently the XHTML format (XML data - HTML formatting) is used or other similar formats, such as MISMO's SMART Doc format or PDF's Intelligent Document, that incorporate the XML data and link it to the content displayed.
Signature Type	Ink signatures for borrowers and notary, documents are then scanned.	Electronic signatures (holographic signing/stylus & signing pad.)	Current adopters are using digital signatures and certificates for signers, notary and recorder. This model supports other forms of electronic signatures.
Security	Virtual Private Network (VPN)	Digital Signatures and Certificate (Closing Agent and Recorder) / SSL (Transmission).	Digital signature and certificate used as a tamper-evident signature for the document and for access control identification for transactions / SSL (Transmission).
Preparer	Title companies, Closing Agents and Lenders scan paper & transmit images.	Title companies, Closing Agents, and Lenders transmit 2 files in one electronic record; document images and XML data.	Currently title companies and lenders adopters prepare electronic documents in XHTML format; it supports preparation in compatible formats that provide the functionality of this model.
Recorder	Traditional processing; but no paper. Recorder examines, records, indexes and archives TIFF images.	Recorder examines, records and archives images; automated indexing by extracting XML data (QO process only).	All processes can be automated, including examination and indexing; or, the recorder can choose manual processing.
Recorded Document	Recorder transmits recorded TIFF ("burned") copy; label data sent also for paper docs.	Recorder transmits recorded image ("burned") to preparer.	Recorder's system adds recording information to the electronic document as XML data for use by the preparer; converts the recorded electronic document to TIFF for archiving.
Payment	"Draw-down" or escrow account for payment.	"Draw-down" or escrow account for payment / ACH transaction.	"Draw-down" or escrow account; debit account' ACH transaction.

Benefits from different eRecording Models

Model 1	Model 2	Model 3
Reduces recording time / Improves the amount of documents processed.	Reduces recording time / Improves throughout	Reduces recording time / Improves throughout
Reduces costs to recorder only.	Reduces costs to the recorder and title company, closing agent, or lender.	Reduces costs to the recorder and title company.
Improves productivity to recording office only.	Improves productivity for both document submitter and recorder.	Improves productivity for both document submitter and recorder.
Improves customer service and satisfaction.	Reduces the probability of documents being altered after transaction is closed/Encrypted "wrapper".	Reduces the probability of documents being altered after transactions is closed/Secure signatures.
	Uses open and non-proprietary systems and formats.	Standardizes processes and formats.
	Improves customer service and satisfaction.	"SMART" documents automate processes and systems.
		Uses open and non-proprietary systems and formats.
		Improves customer service and satisfaction.

Issues concerning different eRecording Models

Model 1	Model 2	Model 3
Complexity of the process of scanning and labeling for submitters	Images are unintelligent	Payment and electronic transaction disconnected/ adds complexity to process.
TIFF image is unintelligent; data is not extractable	Electronic document and XML data are disconnected; possible need for reconciliation.	
Costs increase to submitters; may be greater than or equal to paper	Closed system architecture and proprietary software	
Closed system architecture (proprietary)	Payment and electronic transaction disconnected adds complexity to process	
Payment and electronic transaction disconnected; adds complexity to process	Lacks embedded business rules.	
Cost for proprietary software and data connection	Process and transport are cumbersome.	
Lacks embedded business rules		
Process and transport are cumbersome.		

Appendix D
Related Statutes and Regulations

For the most recent version of the statutes, please click on the hyperlink.

Arizona URPERA: Arizona Uniform Real Property Electronic Recording Act

§ 11-487. Short title

This article may be cited as the uniform real property electronic recording act.

§ 11-487.01. Definitions

In this chapter, unless the context otherwise requires:

1. "Document" means information that is both of the following:

(a) Inscribed on a tangible medium or stored in an electronic or other medium, and retrievable in perceivable form.

(b) Eligible to be recorded in the land records maintained by a county recorder.

2. "Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

3. "Electronic document" means a document that is received by a county recorder in an electronic form.

4. "Electronic signature" means an electronic sound, symbol or process attached to or logically associated with a document and executed or adopted by a person with the intent to sign the document.

5. "Person" means an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, public corporation, government or governmental subdivision, agency or instrumentality or any other legal or commercial entity.

6. "State" means a state of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the United States virgin islands or any territory or insular possession subject to the jurisdiction of the United States.

§ 11-487.02. Validity of electronic documents

A. If a law requires, as a condition for recording, that a document be an original, be on paper or another tangible medium or be in writing, the requirement is satisfied by an electronic document satisfying this article.

B. If a law requires, as a condition for recording, that a document be signed, the requirement is satisfied by an electronic signature.

C. A requirement that a document or a signature associated with a document be notarized, acknowledged, verified, witnessed or made under oath is satisfied if the electronic signature of the person authorized to perform that act, and all other information required to be included, is attached to or logically associated with the document or signature. A physical or electronic image of a stamp, impression or seal need not accompany an electronic signature.

§ 11-487.03. Recording of documents; definition

A. A county recorder:

1. Who implements any of the functions listed in this section shall do so in compliance with adopted standards.

2. May receive, index, store, archive and transmit electronic documents.

3. May provide for access to, and for search and retrieval of, documents and information by electronic means.

4. Who accepts electronic documents for recording shall continue to accept paper documents as authorized by state law and shall place entries for both types of documents in the same index.

5. May convert paper documents accepted for recording into electronic form.

6. May convert into electronic form information recorded before the county recorder began to record electronic documents.

7. May accept electronically any fee that the county recorder is authorized to collect.

8. May agree with other officials of a state or a political subdivision of a state or of the United States, on procedures or processes to facilitate the electronic satisfaction of prior approvals and conditions precedent to recording and the electronic payment of fees.

B. For the purposes of this section, "paper document" means a document that is received by a county recorder in a form that is not electronic.

§ 11-487.04. Uniformity of application and construction

In applying and construing this article, consideration must be given to the need to promote uniformity of the law with respect to its subject matter among states that enact it.

AETA: Arizona Electronic Transactions Act

Article 1. General Provisions

§ 44-7001. Short title
This chapter may be cited as the Arizona electronic transactions act.

§ 44-7002. Definitions

In this chapter, unless the context otherwise requires:

1. "Agreement" means the bargain of the parties in fact, as found in their language or inferred from other circumstances and from rules, regulations and procedures that are given the effect of agreements under laws otherwise applicable to a particular transaction.

2. "Automated transaction" means a transaction that is conducted or performed, in whole or in part, by electronic means or electronic records and in which the acts or records of one or both parties are not reviewed by an individual in the ordinary course in forming a contract, performing under an existing contract or fulfilling an obligation that is required by the transaction.

3. "Computer program" means a set of statements or instructions to be used directly or indirectly in an information processing system in order to bring about a certain result.

4. "Contract" means the total legal obligation resulting from the parties' agreement as affected by this chapter and any other applicable law.

5. "Electronic" means relating to technology that has electrical, digital, magnetic, wireless, optical or electromagnetic capabilities or similar capabilities.

6. "Electronic agent" means a computer program or an electronic or other automated means that is used independently to initiate an action or respond to electronic records or performances, in whole or in part, without review or action by an individual.

7. "Electronic record" means a record that is created, generated, sent, communicated, received or stored by electronic means.

8. "Electronic signature" means an electronic sound, symbol or process that is attached to or logically associated with a record and that is executed or adopted by an individual with the intent to sign the record.

9. "Governmental agency" means an executive, legislative or judicial agency, department, board, commission, authority, institution or instrumentality of the federal government or a state or of a county or municipality or other political subdivision of a state.

10. "Information" means data, text, images, sounds, codes, computer programs, software or databases or similar items.

11. "Information processing system" means an electronic system for creating, generating, sending, receiving, storing, displaying or processing information.

12. "Person" means an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental agency or public corporation or any other legal or commercial entity.

13. "Record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and that is retrievable in perceivable form.

14. "Security procedure" means a procedure that is employed to verify that an electronic signature, record or performance is that of a specific person or to detect changes or errors in the information in an electronic record. Security procedure includes a procedure that requires the use of algorithms or other codes, identifying words or numbers or encryption, callback or other acknowledgment procedures.

15. "State" means a state of the United States, the District of Columbia, Puerto Rico, the United States Virgin Islands or any territory or insular possession subject to the jurisdiction of the United States. State includes an Indian tribe or band or Alaskan native village that is recognized by federal law or formally acknowledged by another state.

16. "State agency" means any department, commission, board, institution or other agency of the state that receives, expends or disburses state funds or incurs obligations of the state, including the Arizona board of regents but excluding the universities under the jurisdiction of the Arizona board of regents, the community college districts and the legislative or judicial branches.

17. "Transaction" means an action or set of actions occurring between two or more persons relating to the conduct of business, commercial or governmental affairs.

§ 44-7003. Scope

A. Except as otherwise provided in subsection B of this section, this chapter applies to any electronic record and electronic signature relating to a transaction.

B. This chapter does not apply to a transaction to the extent the transaction is governed by:

1. Title 14[1] as it relates to the creation and execution of wills, codicils or testamentary trusts.

2. Title 47,[2] other than chapters 2[3] and 2A[4] and § 47-1306 and as otherwise provided in § 44-7016.

[1] Section 14-1101 et seq. (Title 14, Trusts, Estates and Protective Proceedings, Chapter 1, begins in A.R.S. § 11-1402)
[2] Section 47-1101 et seq.
[3] Section 47-2101 et seq.
[4] Section 47-2A101 et seq.

C. This chapter applies to an electronic record or electronic signature otherwise excluded from the application of this chapter under subsection B of this section to the extent the record or signature is governed by a law other than those laws described in subsection B of this section.

D. Any transaction subject to this chapter is also subject to any other applicable substantive law.

§ 44-7004. Prospective application

This chapter applies to any electronic record or electronic signature created, generated, sent, communicated, received or stored on or after the effective date of this chapter.

§ 44-7005. Use of electronic records and signatures; variation by agreement

A. This chapter does not require a record or signature to be created, generated, sent, communicated, received or stored or otherwise processed or used by electronic means or in electronic form.

B. This chapter applies only to transactions between parties each of which has agreed to conduct transactions by electronic means. Whether the parties agree to conduct a transaction by electronic means is determined from the context and surrounding circumstances, including the parties' conduct.

C. A party that agrees to conduct a transaction by electronic means may refuse to conduct other transactions by electronic means. The right granted by this subsection may not be waived by agreement.

D. Except as provided in subsection C and otherwise provided in this chapter, the effect of any of the provisions of this chapter may be varied by agreement. The words "unless otherwise agreed", or other similar words, as used in this chapter do not imply that the effect of other provisions may not be varied by agreement.

E. Whether an electronic record or electronic signature has legal consequences is determined by this chapter and any other applicable law.

§ 44-7006. Construction; application

This chapter shall be construed and applied to:

1. Facilitate electronic transactions consistent with other applicable law.

2. Be consistent with reasonable practices concerning electronic transactions and with the continued expansion of those practices.

3. Effectuate its general purpose to make uniform the law of this state with respect to the subject of this chapter for intrastate, interstate and international transactions.

§ 44-7007. Legal recognition of electronic records, signatures and contracts

A. A record or signature in electronic form cannot be denied legal effect and enforceability solely because the record or signature is in electronic form.

B. A contract formed by an electronic record cannot be denied legal effect and enforceability solely because an electronic record was used in its formation.

C. An electronic record satisfies any law that requires a record to be in writing.

D. An electronic signature satisfies any law that requires a signature.

§ 44-7008. Provision of information in writing; presentation of records

A. If the parties to a transaction have agreed to conduct the transaction by electronic means and a law requires a person to provide, send or deliver information in writing to another person, the requirement is satisfied if the information is provided, sent or delivered, as the case may be, in an electronic record that is capable of retention by the recipient at the time of receipt. An electronic record is not capable of retention by the recipient if the sender or the sender's information processing system inhibits the ability of the recipient to print or store the electronic record.

B. If a law other than this chapter requires a person to post or display a record in a certain manner, to send, communicate or transmit a record by a specified method or to format information in a record in a certain manner, the following requirements apply:

1. The record shall be posted or displayed in the manner prescribed in that law.

2. Except as otherwise provided in subsection D, paragraph 2, the record shall be sent, communicated or transmitted by the method prescribed in that law.

3. The record shall contain the information formatted in the manner prescribed in that law.

C. If a sender inhibits the ability of a recipient to store or print an electronic record, the electronic record is not enforceable against the recipient.

D. The parties to the transaction shall not vary the requirements of this section, except that to the extent a law other than this chapter requires:

1. Information to be provided, sent or delivered in writing but allows that requirement to be varied by agreement, the parties may agree to vary the requirement prescribed in subsection A that the information be in the form of an electronic record capable of retention.

2. A record to be sent, communicated or transmitted by postage prepaid first class mail or regular mail but allows that requirement to be varied by agreement, the parties may agree to vary the requirement to the extent allowed by the other law.

§ 44-7009. Attribution and effect of electronic record and signature

A. An electronic record or electronic signature is attributable to a person if the record or signature was the act of the person or the person's electronic agent. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable.

B. The effect of an electronic record or electronic signature that is attributed to a person under subsection A is determined from the context and surrounding circumstances at the time the record or signature was created, executed or adopted, including the parties' agreement, if any, and as otherwise provided by law.

§ 44-7010. Effect of change or error

A. The following apply to any change or error in an electronic record that occurs in a transmission between the parties to a transaction:

1. If the parties have agreed to use a security procedure to detect changes or errors and one party has conformed to the procedure but the other party has not, and the nonconforming party would have detected the change or error had that party also conformed, the conforming party may avoid the effect of the changed or erroneous electronic record.

2. In an automated transaction that involves an individual, the individual may avoid the effect of an electronic record that resulted from an error made by the individual in dealing with the electronic agent of another person if the electronic agent did not provide an opportunity for the prevention or correction of the error and, at the time the individual learns of the error, the individual:

(a) Promptly notifies the other person of the error and that the individual did not intend to be bound by the electronic record received by the other person.

(b) Takes reasonable steps, including steps that conform to the other person's reasonable instructions, to return to the other person or, if instructed by the other person, to destroy the consideration received, if any, as a result of the erroneous electronic record.

(c) Has not used or received any benefit or value from the consideration, if any, received from the other person.

B. If subsection A, paragraphs 1 and 2 do not apply, the change or error has the effect provided by other applicable law, including the law of mistake, and the parties' contract, if any.

C. The parties to the transaction shall not agree to vary the requirements prescribed in subsection A, paragraph 2 and subsection B.

§ 44-7011. Notarization; acknowledgment

Notwithstanding title 41, chapter 2, article 2, if the law requires a signature or record to be notarized, acknowledged, verified or made under oath, that requirement is satisfied if a notary completes a notarial act on the electronic message or document. That notarial act on the electronic message or document is complete without the imprint of the notary's seal if all of the following apply:

1. The electronic message or document is signed pursuant to this chapter or § 41-132 in the presence of a notary.

2. The notary confirms that the electronic signature on the electronic message or document is verifiably the electronic signature issued to the signer pursuant to this chapter or § 41-132.

3. The notary electronically signs with an electronic signature that is consistent with this chapter, any electronic notary law or any other applicable law.

4. The following information appears electronically within the message electronically signed by the notary:

(a) The notary's full name and commission number exactly as it appears on the notary's commission.

(b) The words "electronic notary public", "state of Arizona" and "my commission expires on (date)".

(c) The address of the notary's principal place of contact exactly as it appears on the notary's commission.

(d) The notary's E-mail or other electronic address exactly as it appears on the notary's commission.

§ 44-7012. Electronic records retention; originals

A. If a law requires that a record be retained, the requirement is satisfied by retaining an electronic record of the information in the record that:

1. Accurately reflects the information prescribed in the record after the record was first generated in its final form as an electronic record or otherwise.

2. Remains accessible for later reference.

B. Subsection A does not apply to any information whose sole purpose is to enable the record to be sent, communicated or received.

C. A person may satisfy subsection A by using the services of another person to satisfy subsection A.

D. If a law requires:

1. A record to be presented or retained in its original form, or provides consequences if the record is not presented or retained in its original form, that law is satisfied by an electronic record retained according to subsection A.

2. Retention of a check, that requirement is satisfied by retention of an electronic record of the information on the front and back of the check according to subsection A.

E. A record Retained as an electronic record pursuant to subsection A satisfies a law that requires a person to retain a record for evidentiary, audit or like purposes, unless a law that is enacted after the effective date of this chapter prohibits the use of an electronic record for the specified purpose.

F. This section does not prohibit a governmental agency from adopting additional requirements for the retention of a record that is subject to that agency's jurisdiction.

§ 44-7013. Admissibility in evidence

In any proceeding, evidence of a record or signature may not be excluded solely because it is in electronic form.

§ 44-7014. Automated transaction contracts

A. In any automated transaction, the parties may form a contract by the interaction of:

1. Electronic agents of the parties, even if no individual was aware of or reviewed the electronic agents' actions or the resulting terms and agreements.

2. An electronic agent and an individual who acts on the individual's own behalf or for another person, including by an interaction in which the individual performs actions that the individual may refuse to perform and in which the individual knows or has reason to know will cause the electronic agent to complete the transaction or performance.

B. In addition to subsection A, paragraphs 1 and 2, the terms of any contract are determined by the substantive law that applies to that contract.

§ 44-7015. Time and place of sending and receipt

A. Unless otherwise agreed to by the sender and the recipient, an electronic record is sent if the record:

1. Is properly addressed or otherwise properly directed to an information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record.

2. Is in a form that is capable of being processed by the information processing system described in paragraph 1 of this subsection.

3. Enters an information processing system that is outside the control of the sender or of a person that sent the electronic record on behalf of the sender or enters a region of the information processing system that is designated or used by the recipient and that is under the control of the recipient.

B. Unless otherwise agreed to by the sender and the recipient, an electronic record is received if the record:

1. Enters an information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record.

2. Is in a form that is capable of being processed by the information processing system described in paragraph 1 of this subsection.

C. Subsection B applies even if the information processing system is located in a different place from the place the electronic record is deemed to be received pursuant to subsection D.

D. Unless otherwise expressly provided in the electronic record or agreed to by the sender and the recipient, an electronic record is deemed to be sent from the sender's place of business and to be received at the recipient's place of business. If the sender or recipient has more than one place of business, the place of business of that person is the place that has the closest relationship to the underlying transaction. If the sender or the recipient does not have a place of business, the place of business is the sender's or recipient's residence, as applicable.

E. An electronic record is received pursuant to subsection B even if no individual is aware of its receipt.

F. Receipt of an electronic acknowledgment from an information processing system described in subsection B establishes that a record was received but, by itself, does not establish that the content sent corresponds to the content received.

G. If a person is aware that an electronic record was purportedly sent as prescribed in subsection A or purportedly received as prescribed in subsection B, but was not actually sent or received,

the legal effect of the sending or receipt is determined by other applicable law. Except to the extent allowed by the other law, the parties may not agree to vary the requirements of this subsection.

§ 44-7016. Transferable records; definition

A. A person has control of a transferable record if a system employed for evidencing the transfer of interests in the transferable record reliably establishes that person as the person to which the transferable record was issued or transferred.

B. A system complies with subsection A and a person has control of a transferable record if the transferable record is created, stored and assigned in such a manner that all of the following are true:

1. A single authoritative copy of the transferable record exists that is unique, identifiable and, except as otherwise provided in paragraphs 4, 5 and 6 of this subsection, unalterable.

2. The authoritative copy identifies the person asserting control as either:

(a) The person to which the transferable record was issued.

(b) If the authoritative copy indicates that the transferable record has been transferred, the person to which the transferable record was most recently transferred.

3. The authoritative copy is communicated to and maintained by the person asserting control or the person's designated custodian.

4. Copies or revisions that add or change an identified assignee of the authoritative copy can be made only with the consent of the person asserting control.

5. Each copy of the authoritative copy and any copy of a copy is readily identifiable as a copy that is not the authoritative copy.

6. Any revision of the authoritative copy is readily identifiable as authorized or unauthorized.

C. Except as otherwise agreed, a person that has control of a transferable record is the holder as defined in § 47-1201 of the transferable record and has the same rights and defenses as a holder of an equivalent record or writing pursuant to title 47 including, if the applicable requirements under § 47- 3302, subsection A or § 47-7501 or 47-9308 are satisfied, the rights and defenses of a holder in due course, a holder to which a negotiable document of title has been duly negotiated or a purchaser, respectively. Delivery, possession and indorsement are not required to obtain or exercise any of the rights under this subsection.

D. Except as otherwise agreed, an obligor under a transferable record has the same rights and defenses as an equivalent obligor under equivalent records or writings under title 47.

E. If requested by a person against which enforcement is sought, the person seeking to enforce the transferable record shall provide reasonable proof that the person is in control of the transferable record. Proof may include access to the authoritative copy of the transferable record and related business records that are sufficient to review the terms of the transferable record and to establish the identity of the person that has control of the transferable record.

F. For the purposes of this section, "transferable record" means an electronic record that both:

1. Would be a note pursuant to title 47, chapter 3 or a document pursuant to title 47, chapter 7 if the electronic record were in writing.

2. The issuer has expressly agreed the electronic record is a transferable record.

Article 2. Secure Electronic Records and Signatures

§ 44-7031. Secure electronic signatures

A signature is a secure electronic signature if, through the application of a security procedure, it can be demonstrated that the electronic signature at the time the signature was made was all of the following:

1. Unique to the person using it.

2. Capable of verification.

3. Under the sole control of the person using it.

4. Linked to the electronic record to which it relates in such a manner that if the record were changed the electronic signature would be invalidated.

§ 44-7032. Secure electronic records

If, through the ongoing application of a security procedure, it can be demonstrated that an electronic record signed by a secure electronic signature has remained unaltered since a specified time, the record is a secure electronic record from that time of signing forward.

§ 44-7033. Presumptions

A. There is a rebuttable presumption that a secure electronic record has not been altered since the specific time to which the secure status relates.

B. There is a rebuttable presumption that the secure electronic signature is the electronic signature of the party to whom it relates.

C. In the absence of a secure electronic record or a secure electronic signature, this chapter does

not create any presumption regarding the authenticity and integrity of an electronic record or an electronic signature.

§ 44-7034. Electronic notarization; acknowledgment

If a law requires a signature or record to be notarized, acknowledged, verified or made under oath, that requirement is satisfied if all of the following are true:

1. A secure electronic signature of the individual who is authorized to perform those acts and all other information that is required to be included pursuant to any other applicable law are applied to a secure electronic record.

2. The secure electronic record has a time stamp token that is both:

(a) Created by a party recognized by the secretary of state.

(b) in a form that is accepted by the secretary of state to do all of the following:

(i) Reasonably verify the validity of the signing party's secure electronic signature.

(ii) Reasonably establish the time of signing.

3. The secure electronic record cannot be altered without invalidating the time stamp token.

Article 3. Governmental Electronic Records

§ 44-7041. Creation; retention; conversion of written records

A. Each governmental agency shall determine if, and the extent to which, the governmental agency will create and retain electronic records and convert written records to electronic records. Any governmental agency that is subject to the management, preservation, determination of value and disposition of records requirements prescribed in §§ 41-1345, 41-1345.01 and 41-1346 through 41-1351 and the permanent public records requirements prescribed in § 39-101 shall comply with those requirements.

B. State agencies shall comply with the standards adopted by the government information technology agency pursuant to title 41, chapter 32.

C. All governmental agencies shall comply with the policies that are established by the secretary of state pursuant to § 41-132 and that apply to the use of electronic signatures.

§ 44-7042. Sending and accepting electronic records

A. Except as otherwise provided in § 44-7012, subsection E, each governmental agency shall determine if, and the extent to which, the governmental agency will send and accept electronic records and electronic signatures to and from other persons and otherwise create, generate, communicate, store, process, use and rely on electronic records and electronic signatures. State

agencies shall comply with the appropriate standards and policies adopted or established by the government information technology agency pursuant to title 41, chapter 32 and the secretary of state pursuant to § 41-132.

B. To the extent that a governmental agency uses electronic records and electronic signatures pursuant to subsection A of this section, the governmental agency after giving due consideration to security may specify:

1. The manner and format in which the electronic records must be created, generated, sent, communicated, received and stored and the systems established for those purposes.

2. If electronic records must be signed by electronic means, the type of electronic signature required, the manner and format in which the electronic signature must be affixed to the electronic record and the identity of or criteria that must be met by any third party used by a person filing a document to facilitate the process.

3. Control processes and procedures as appropriate to ensure adequate preservation, disposition, integrity, security, confidentiality and ability to perform audits of electronic records.

4. Any other required attributes for electronic records that are specified for corresponding non-electronic records or that are reasonably necessary under the circumstances.

C. Except as otherwise provided in § 44-7012, Subsection E, this chapter does not require a governmental agency to use or allow the use of electronic records or electronic signatures.

§ 44-7043. Interoperability

Technology standards adopted by the governmental information technology agency, electronic signature use policies adopted by the secretary of state or any other similar standards adopted by any other governmental agency pursuant to § 44-7042 shall encourage and promote consistency and interoperability with similar requirements adopted by other governmental agencies, other states, the federal government and nongovernmental persons that interact with governmental agencies. If deemed appropriate by the entity adopting the standards, the standards may allow for differing levels of standards from which governmental agencies may choose in implementing the most appropriate standard for a particular application.

Article 4. Miscellaneous Provisions

§ 44-7051. Consumer protection

A. Nothing in this chapter diminishes the parties' consumer protection rights prescribed in chapter 10, article 7 of this title or any other federal or state law relating to consumers.

B. If a consumer law, other than this chapter, requires a paper record or notice of the transaction, the parties to the transaction may request that the record or notice be provided in an electronic format and that record or notice shall comply with this chapter. Even if before completing a consumer transaction by an electronic method that complies with this chapter, a party to the

transaction requests that a record or notice of the transaction be delivered in electronic form, that party may subsequently change that preference and request that all future records or notices relating to that transaction be sent in paper form to an appropriate address. Withdrawal of consent does not affect the enforceability of electronic records or notices previously provided or made available to that party in accordance with this chapter.

C. A nonelectronic consumer contract or agreement may not contain a provision that authorizes any transaction or part of any transaction pursuant to that contract or agreement by electronic means unless all of the following apply:

1. The consumer makes a separate and express assent or signing either manually or electronically that specifies that the consumer agrees that certain transactions or parts of transactions will be conducted by electronic means.

2. The contract or agreement indicates which transactions or parts of transactions that may be conducted by electronic means and the manner in which those transactions or parts of transactions shall be conducted.

3. The consumer agrees, as part of the assent, to provide the other party with the consumer's electronic address that complies with § 44-7015.

4. The consumer agrees, as part of the assent, to notify the other party, either manually or electronically, of any change in the electronic address prescribed in paragraph 3 or the consumer's withdrawal of consent to electronic transactions.

Electronic Signatures Administrative Regulations

Arizona Administrative Code R2-12-501 through R2-12-504

R2-12-501. Definitions

A. "Acceptable Certification Authorities" means authorities that meet the requirements of R2-12-504.

B. "Approved List of Certification Authorities" means the list of Certification Authorities approved by the Secretary of State to issue certificates for electronically signed transactions involving public entities in Arizona.

C. "Asymmetric crypto-system" means an electronically processed algorithm, or series of algorithms, which uses two different keys with the following characteristics:

1. One key encrypts a given message;
2. One key decrypts a given message; and
3. The keys have the property that it is infeasible to discover one key from merely knowing the other key.

D. "CARAT Guidelines" means the *CARAT Guidelines - Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates* drafted by the Certification Authority Rating and Trust (CARAT) Task Force of the National Automated Clearing House Association (NACHA), Version 1 Draft, September 21, 1998, excluding later amendments or additions, incorporated by reference and on file with the Secretary of State.

E. "Certificate" means an electronic document attached to a public key by a trusted certification authority, which provides proof that the public key belongs to a legitimate subscriber and has not been compromised.

F. "Certification Authority" means a person or entity that issues a certificate.

G. "Electronically signed communication" means an electronic message that has been processed in such a manner that the message is tied to the individual who signed the message.

H. "GITA" means the Government Information Technology Agency, as established by A.R.S. § 41-3501.

I. "Key pair" means a private key and its corresponding public key in an asymmetric crypto-system. The key pair is unique in that the public key can verify a digital signature that the private key creates.

J. "Message" means an electronic representation of information intended to serve as a written communication with a public entity.

K. "Person" means a human being or any organization capable of signing a document, either legally or as a matter of fact.

L. "Policy Authority" means, as defined by CARAT Guidelines, some authoritative party that formulates the guidelines defining the process of electronic signature use.

M. "Private key" means the key of a key pair used to create a digital signature.

N. "Public key" means the key of a key pair used to verify a digital signature.

O. "Public entity" means any budget unit, as defined in A.R.S. § 41-3501.

P. "S.A.S. 70" means the standards set in the American Institute of Certified Public Accounts (AICPA) Statement on Auditing Standards No. 70. Should current S.A.S. 70 standards (or any succeeding version) be superceded, the Secretary of State, in consultation with GITA and the State Treasurer, shall establish a deadline for all affected parties to comply with the replacing standard. This deadline shall be no later than two years from the date of issuance of the new S.A.S. standards. GITA will also provide a "roadmap" of how the revised standard fits the current Type 1 and Type 2 S.A.S. 70 designations used elsewhere in these rules.

Q. "Subscriber" means a person who:
1. Is the subject listed in a certificate,
2. Accepts the certificate, and
3. Holds a private key which corresponds to a public key listed in that certificate.

R2-12-502. Identification of Acceptable Technologies for Electronic Signatures

A. The Secretary of State shall accept, and approve for use, technologies for electronic signature, in consultation with the Policy Authority and GITA, provided the technologies meet the standards set forth in the GITA standards for Electronic Signatures, as specified in A.R.S. § 41-3504.

B. Provisions for Adding New Technologies
1. Any individual or company can petition the Secretary of State to review the technology, by providing a written request for review including a full explanation of a proposed technology that meets the requirements established under subsection (A) and meets the requirements of the Policy Authority as identified in R2-12-503.
2. The Secretary of State has 180 days from the date of the request to review the petition and either accept or reject it.
   a. If the petitioner's proposed technology meets the requirements established under subsection (A) and meets the requirements of the Policy Authority, then GITA shall work with the Policy Authority to incorporate the new technology into electronic signature use by public agencies in Arizona.
   b. If the proposed technology is rejected, the petitioner can appeal the decision through the Administrative Procedure Act, A.R.S. § 41-1092.08(H).

R2-12-503. Policy Authority

A. The office of the Secretary of State shall serve as the Policy Authority as defined within the CARAT Guidelines. These guidelines provide a prudent operational model that may be applied to new technologies as they are approved.

B. Decisions made by the Policy Authority under R2-12-501, R2-12-502, and R2-12-504 may be appealed pursuant to the Administrative Procedure Act, A.R.S. § 41-1092.08(H).

R2-12-504. Certification Authority Approval Application, Suspension, Revocation

A. Acceptable Certification Authorities
1. The Secretary of State shall maintain an "Approved List of Certification Authorities" authorized to issue certificates for electronically signed communication with public entities in Arizona.
2. Public entities shall only accept certificates from Certification Authorities that appear on the "Approved List of Certification Authorities" and are authorized to issue certificates by the Secretary of State.

B. Registration of Certification Authorities
1. The Secretary of State shall place Certification Authorities on the "Approved List of Certification Authorities" after the Certification Authority provides the Secretary of State with a copy of an unqualified performance audit performed in accordance with standards set in S.A.S. 70 to ensure that the Certification Authorities practices and policies are consistent with the requirements in this Article and any requirements of the Policy Authority.

a. Certification Authorities that have been in operation for one year or less shall undergo a S.A.S. 70 type 1 audit - A report of Policies and Procedures placed in operation, receiving an unqualified opinion.
b. Certification Authorities that have been in operation for longer than one year shall undergo a S.A.S. 70 type 2 audit - A Report of Policies and Procedures placed in operation and test of operating effectiveness, receiving an unqualified opinion.
c. To remain on the "Approved List of Certification Authorities", a Certification Authority must provide proof of compliance every two years after initially being placed on the list and meet any requirements of the Policy Authority in effect at that time.

2. In lieu of completing the auditing requirement in subsection (B)(1), Certification Authorities may be placed on the "Approved List of Certification Authorities" upon providing the Secretary of State with proof acceptable to the Secretary of State that the Certification Authority meets the Policy Authority's criteria for acceptance of a Foreign License (non-Arizona license).
   a. Certification Authorities shall be removed from the "Approved List of Acceptable Certification Authorities" unless they provide current proof of accreditation to the Secretary of State at least once per year no later than December 31 of each year.
   b. If the Secretary of State is informed a Certification Authority has had its accreditation revoked, the Certification Authority shall be removed from the "Approved List of Certification Authorities" immediately.

Electronic Notary Statutes and Administrative Regulations

§ 41-351. Definitions

In this article, unless the context otherwise requires:

1. "Approved time stamp provider" means a person or organization recognized by the secretary of state as capable of reliably providing time stamp services on notary service electronic documents.

2. "Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

3. "Electronic acknowledgment" means a notarial act in which an electronic notary electronically certifies that the signer, whose identity is proven by satisfactory evidence, either:

(a) Appeared before the electronic notary and acknowledged that the signer executed the instrument.

(b) Provided secure electronic acknowledgment that the signer executed the electronic instrument presented to the electronic notary.

4. "Electronic commission" means the written authority to perform electronic notarization acts.

5. "Electronic document" means any record created, generated, sent, communicated, received or stored by electronic means.

6. "Electronic jurat" means an electronic notarial act in which the electronic notary certifies that a signer, whose identity is proven by satisfactory evidence, has made in the electronic notary's presence a voluntary electronic signature or mark and has taken an oath or affirmation vouching for the truthfulness of the signed electronic document.

7. "Electronic notary public" or "electronic notary" means any person commissioned to perform notarial acts under this article.

8. "Electronic notary token" means the electronic attachment to a notarized electronic document that is attached by the electronic notary and that contains the notary's electronic signature. The electronic notary token is linked to the electronic document to which it relates in a manner so that if the document is changed the electronic notary token is invalidated.

9. "Electronic signature" means an electronic method or process that through the application of a security procedure allows a determination that the electronic signature at the time it was executed was all of the following:

(a) Unique to the person using it.

(b) Capable of verification.

(c) Under the sole control of the person using it.

(d) Linked to the electronic document to which it relates in a manner so that if the document is changed the electronic signature is invalidated.

10. "Notary service electronic certificate" means the materials and methods issued by an electronic notary to a prospective signer so that signer may create a notary service electronic signature.

11. "Notary service electronic signature" means an act completed by a signer using a properly issued notary service electronic certificate to sign an electronic document.

12. "Oath" or "affirmation" means an act in which a person makes a vow in the presence of the electronic notary under penalty of perjury, with reference made to a supreme being in the case of an oath.

13. "Personal knowledge of identity" means familiarity with an individual resulting from interactions with that individual over a sufficient time to eliminate reasonable doubt that the individual has the identity claimed.

14. "Satisfactory evidence of identity" means that proof of identity is evidenced by one of the following:

(a) At least one current form of identification issued by a federal, state or tribal government with the individual's photograph, signature and written physical description.

(b) The oath or affirmation of a credible person who is personally known to the electronic notary and who personally knows the individual signer.

(c) The oath or affirmation of a credible person who personally knows the individual and who provides satisfactory evidence of identity pursuant to subdivision (a) of this paragraph.

(d) Personal knowledge of the individual signer by the electronic notary.

(e) For the purposes of a real estate conveyance or financing, a valid unexpired passport that is issued by the United States government or any other national government. A passport issued by a national government other than the United States government must be accompanied by a valid visa or other documentation issued by the United States government necessary to establish an individual's legal presence in the United States.

15. "Time stamp token" means a secure electronic method to affix a statement of the time and date that the document was recognized as a valid notary service electronic document by an approved time stamp provider. A time stamp token is attached by an approved time stamp provider to the document in a way that if the document changes the time stamp token is

invalidated.

§ 41-352. Applicability of article; electronic signature laws

A. Any notarial act in which a person by oath or affirmation signs a document may be performed electronically as prescribed by this article if under applicable law that document may be signed with an electronic signature.

B. Unless otherwise expressly prohibited by law, The following notarial acts, terms and entities have the same legal effect as those prescribed by article 2 of this chapter[5]:

1. Electronic acknowledgment as acknowledgment.

2. Electronic oath as oath.

3. Electronic jurat as jurat.

4. Electronic affidavit as affidavit.

5. Electronic notarial act as notarial act.

6. Electronic notarial certificate token as notarial certificate.

7. Electronic notary as notary.

C. An electronic commission is a commission to perform only electronic notary acts and only an electronic notary is authorized to perform electronic notary acts.

D. Unless otherwise expressly prohibited by law, any electronic notarial act may be performed by either:

1. An act in the presence of an electronic notary as prescribed by this article.

2. An electronic notarial service as prescribed by this article for which the person signing appears before an electronic notary and by oath or affirmation acknowledges that any notary service electronic document that is created by the person pursuant to this article has the same legal force and effect as if the person appeared before an electronic notary and by oath or affirmation executed an electronic notarial act.

E. Section 41-132 applies in conjunction with this article to electronic signatures used by electronic notaries.

F. this article applies to electronic notarial acts that are performed by electronic notaries who are

[5] Section 41-311 et seq.

appointed in this state and applies only to their acts performed in the United States.

§ 41-353. Appointment; term; bond; duties

A. The secretary of state may appoint electronic notaries public to hold office for four years.

B. The secretary of state shall prescribe the application form for an electronic notary. Applicants shall submit the application to the secretary of state with a filing fee, a bond and a bond filing fee as prescribed by rule by the secretary of state.

C. The materials and methods for creating notary service electronic certificates and any other encryption based technologies used by an electronic notary shall have a maximum useful life of two years and shall not exceed the life of the electronic notary commission.

D. An electronic notary public is a public officer commissioned by this state and the following apply without regard to whether the electronic notary public's employer or any other person has paid the fees and costs for the commissioning of the electronic notary public, including costs for the materials and methods employed with the electronic notary token and the materials and methods for creating notary service electronic certificates and journals:

1. All of the following remain the property of the electronic notary:

(a) The materials and methods employed with and solely for the electronic notary token.

(b) The materials and methods used solely for creating notary service electronic certificates.

(c) Any journals containing only public information record entries.

2. Notwithstanding paragraph 1 of this subsection, an electronic notary does not gain ownership or presumptive access rights to any of an employer's assets or resources that are used or are usable for a purpose other than electronic notarial acts.

3. An electronic notary may perform electronic notarizations outside the workplace of the electronic notary's employer except during those times normally designated as the electronic notary's hours of duty for that employer. All fees received by an electronic notary for electronic notarial services provided while not on duty remain the property of the electronic notary.

4. An employer of an electronic notary shall not limit the electronic notary's services to customers or other persons designated by the employer.

E. An electronic notary public shall continue to serve until the electronic notary's commission expires, the electronic notary resigns the commission, the electronic notary dies or the secretary of state suspends or revokes the commission. An employer shall not cancel the electronic notary bond or electronic notary commission of any electronic notary who is an employee and who leaves that employment.

F. An electronic notary shall comply with all of the following:

1. Be at least eighteen years of age.

2. Be a resident of this state for income tax purposes and claim the individual's residence in this state as the individual's primary residence on state and federal tax returns.

3. Except as provided in § 41-368, subsection A, paragraph 2, never have been convicted of a felony.

4. Keep as a reference a manual that is approved by the secretary of state and that describes the duties, authority and ethical responsibilities of electronic notaries public.

G. An applicant for appointment and commission as an electronic notary shall complete an application form prescribed by the secretary of state. Except for the applicant's name, physical business address, electronic business address and business telephone number, all other information on the application is confidential and shall not be disclosed to any person other than the applicant, the applicant's personal representative or an officer or employee of the federal government or this state or its political subdivisions who is acting in an official capacity. The secretary of state shall use the information contained on the application only for carrying out the purposes of this article.

H. The state or any of its political subdivisions may pay the fees and costs for the commissioning of an electronic notary who is an employee of this state or any of its political subdivisions and performs electronic notarial services in the course of the electronic notary's employment or for the convenience of public employees.

§ 41-354. Notarized electronic documents; elements

A. A notarized electronic document consists of the following:

1. A complete electronic document.

2. A signature or mark that is affixed to the document by the signer.

3. A time and date statement that is affixed to the document in a manner that is approved by the secretary of state.

4. An electronic notary token that is affixed to the document in a manner that is approved by the secretary of state.

B. On completion of the notarized electronic document, any change to any of the elements prescribed in subsection A invalidates the notarized electronic document.

§ 41-355. Duties; electronic notarization in presence of electronic notary

A. Electronic notaries public shall perform the following electronic notarial acts when requested:

1. Take electronic acknowledgments.

2. Administer oaths and affirmations relating to electronic documents and electronic notarial acts.

3. Perform jurats relating to electronic documents and electronic notarial acts.

4. Educate notary service electronic signature certificate applicants about the responsibilities and consequences of the use of the certificate.

5. Administer an oath or affirmation that the notary service electronic signature certificate applicant understands the responsibilities and consequences of using a notary service electronic signature certificate to sign a notary service electronic document and that the electronic signature certificate has the same legal force and effect as any notarial act made before a notary public pursuant to article 2 of this chapter.[6]

6. Register the notary service electronic signature certificate applicant for the issuance of a notary service electronic signature certificate that has a maximum useful life of two years.

B. A notarized electronic document that is completed in the presence of an electronic notary consists of the following:

1. A complete electronic document.

2. A signature or mark that is affixed to the document by the signer.

3. A time and date statement that is contained within the electronic notary token.

4. An electronic notary token that is affixed by the electronic notary to the document.

C. On completion of the notarized electronic document, any change to any of the elements prescribed in subsection B of this section invalidates the notarized electronic document.

D. An electronic notary public shall:

1. Keep, maintain and protect as a public record a journal of all official acts performed by the notary as prescribed in section 41-361 and in the form prescribed by the secretary of state.

2. Provide and keep the materials and processes to create an electronic notary token as approved

[6] Section 41-311 et seq.

by the secretary of state.

3. Authenticate with the electronic notary token all official acts and affix the date of the expiration of the notary's commission as an electronic notary on every document that the electronic notary electronically signs.

4. Respond to any requests for information and comply with any investigations that are initiated by the secretary of state or the office of the attorney general.

§ 41-356. Electronic notarization without presence of electronic notary

A. An electronic notary may issue a notary service electronic certificate to a signer who does all of the following:

1. Provides satisfactory evidence of the signer's identity.

2. Voluntarily signs or makes the signer's mark on the electronic document.

3. Makes an oath or affirmation that vouches for the truthfulness of the signing.

4. Acknowledges that the electronic signing and oath or affirmation have the same legal force and effect as if done in the presence of the notary.

B. A notary service electronic certificate shall include the agreement of the signer to use the certificate for signing an electronic document with notarial intent.

C. A notarized electronic document formed by the use of a notary service electronic certificate consists of the following:

1. A complete electronic document.

2. A notary service electronic signature that is affixed to the document by the signer.

3. A time stamp token that is affixed to the document by an approved time stamp token provider.

4. An electronic notary token that is incorporated into the notary service electronic signature and that is used by the signer in a manner approved by the secretary of state.

D. On completion of the notarized electronic document, any change to any of the elements prescribed in subsection C invalidates the notarized electronic document.

E. On proper issuance and receipt of a notary service electronic certificate, execution of the electronic signature, attachment of the notary token and attachment and validation of the time stamp token, a notary service electronic document is fully executed and valid for those purposes that allow the use of a notary service electronic document.

§ 41-357. Bond

A. A person who has been commissioned as an electronic notary shall file an oath of office and a bond with the secretary of state. A licensed surety shall execute the bond. The bond is effective for four years beginning on the commission's effective date.

B. The secretary of state shall not accept any bond that was issued more than sixty days before or more than thirty days after the date on which the secretary of state commissions an electronic notary.

§ 41-358. Fees; rules

A. Electronic notaries public may receive fees for the following services:

1. Acknowledgments.

2. Oaths and affirmations.

3. Jurats.

4. Issuance of notary service electronic certificates.

B. The secretary of state shall determine by rule fees for services.

§ 41-359. Delivering notarial journals and records; failure to comply; civil penalty; storing records; certified copies

A. On the resignation or revocation of an electronic notarial commission, the death of a notary or the expiration of an electronic commission, the electronic notarial journal and records, except those records of notarial acts that are not public record, shall be delivered by certified mail or other means providing a receipt to the office of the secretary of state. if an electronic notary does not apply for reappointment, on expiration of the notarial commission the journal and records shall be delivered to the secretary of state as required for resignation under this subsection. If an electronic notary or the personal representative of a deceased electronic notary does not deposit these records and papers within three months of the expiration of the commission, the secretary of state shall order the notary or the notary's personal representative to pay a civil penalty of at least fifty dollars but not more than five hundred dollars.

B. While an electronic notary public is commissioned, an electronic notary public shall keep all records and journals of the notary's acts for at least five years after the date the electronic notarial act was performed. On receipt of the records and journals from an electronic notary public who no longer is commissioned, the secretary of state shall keep all records and journals of electronic notaries public deposited in the secretary of state's office for five years and shall give certified copies when required, and for the copy certifications the secretary of state shall receive the same fees allowed by law to electronic notaries public pursuant to § 41-358. The copy certifications are as valid and effective as if given by an electronic notary public.

§ 41-360. Destruction of records; penalty

Any person who knowingly destroys, defaces or conceals any journal entry or records belonging to the office of an electronic notary public shall forfeit to the state not more than five hundred dollars and is liable for damages to any injured party.

§ 41-361. Journal; confidential records

A. The electronic notary shall keep or shall contract with a party that complies with procedures established by the secretary of state to keep a journal in a form approved by the secretary of state. The electronic notary shall record all notarial acts in chronological order. The electronic notary shall furnish, when requested, a certified copy of any specific public record in the notary's journal. Records of notarial acts that violate the attorney-client privilege or that are confidential pursuant to federal law or the laws of this state are not public record. Each journal entry shall include at least:

1. The date of the electronic notarial act.

2. A description of the document date, time and type of electronic notarial act.

3. The full name and address of each person for whom an electronic notarial act is performed and a description of the verification of the signer's mark.

4. The type of satisfactory evidence of identity presented to the electronic notary by each person for whom an electronic notarial act is performed.

5. A description of the identification document, its serial or identification number and its date of issuance or expiration.

6. The fee, if any, charged for the electronic notarial act.

B. If an electronic notary has personal knowledge of the identity of a signer, the requirements of subsection A, paragraphs 1 through 5 may be satisfied by the notary retaining a paper or electronic copy of the electronic notarized documents for each electronic notarial act.

C. If an electronic notary does more than one notarization for an individual within a six month period, the electronic notary shall have the individual provide satisfactory evidence of identity the first time the electronic notary performs the notarization for the individual but need not require satisfactory evidence of identity or the individual to sign the journal for subsequent notarizations performed for the individual during the six month period.

D. Except as provided in subsection A, the electronic notary's journal is a public record that may be viewed by or copied for any member of the public, but only on presentation to the notary of a written request that details the month and year of the electronic notarial act, the name of the person whose signature was notarized and the type of document or transaction. An electronic

notary shall provide a copy of the requested entry in a form the secretary of state prescribes by rule.

§ 41-362. Competency of corporation notaries

A. An electronic notary public who is a stockholder, director, officer or employee of a corporation may do any of the following:

1. Take the acknowledgment or oath of any party to any written instrument executed to or by the corporation.

2. Administer an oath to any other stockholder, director, officer, employee or agent of the corporation.

3. Protest for nonacceptance or nonpayment of bills of exchange, drafts, checks, notes and other negotiable instruments that the corporation owns or holds for collection.

B. An electronic notary public shall not do any of the following:

1. Take the acknowledgment of an instrument executed by or to a corporation of which the electronic notary is a stockholder, director, officer or employee, if the notary is a party to the instrument, either individually or as a representative of the corporation.

2. Protest any negotiable instrument that the corporation owns or holds for collection, if the notary is individually a party to the instrument.

§ 41-363. Authentication of authority of officer for foreign notarizations

An electronic notarial act performed by any of the persons described in § 33-501 shall be recognized in this state if the notarial act creates an electronically notarized electronic document as prescribed by this article.

§ 41-364. Change of address; lost or stolen electronic journal or seal; civil penalty

A. Within thirty days after the change of an electronic notary's mailing, residential or electronic address, the electronic notary shall deliver to the secretary of state, by certified mail or other means providing a receipt, a signed notice of the change that provides both the old and new addresses.

B. Within ten days after the loss or theft of an official journal or any materials or processes used in creating an electronic notary token or registering notary service electronic certificate applicants, the electronic notary shall deliver to the secretary of state, by certified mail or other means providing a receipt, a signed notice of the loss or theft. The electronic notary also shall inform the appropriate law enforcement agency in the case of theft.

C. If an electronic notary fails to comply with subsection A or B, the electronic notary has failed to fully and faithfully discharge the duties of an electronic notary and the secretary of state may impose against the electronic notary a civil penalty in an amount the secretary of state prescribes by rule. The electronic notary shall pay any civil penalty imposed by the secretary of state pursuant to this subsection before the renewal of the notary's commission.

§ 41-365. Name change; new commission; failure to comply

A. An electronic notary whose name changes shall apply for new methods and materials issued to the electronic notary to create electronic notary tokens under the new name.

B. An electronic notary shall notify the secretary of state within thirty days after the notary's change of name. If the electronic notary fails to comply with this subsection, the electronic notary has failed to fully and faithfully discharge the duties of an electronic notary.

§ 41-366. Prohibited conduct; incomplete documents; signatures of relatives

A. An electronic notary public shall not perform an electronic jurat on a document that is incomplete. If an electronic notary public is presented with a document that the electronic notary knows from experience to be incomplete or if the document on its face is incomplete, the electronic notary public shall refuse to perform the jurat.

B. An electronic notary public is an impartial witness and shall not notarize the notary's own signature or the signatures of any person who is related by marriage or adoption.

§ 41-367. Electronic notary public title; foreign language; violation; classification

A. Every electronic notary public who is not an attorney and who advertises, by any written or verbal means, the services of an electronic notary public in a language other than English, with the exception of a single desk plaque, shall post or otherwise include with the advertisement a notice in English and the other language. The notice shall be in of conspicuous size, if in writing, and shall state: "I am not an attorney and cannot give legal advice about immigration or any other legal matters."

B. An electronic notary public who violates subsection A is guilty of a class 6 felony and the secretary of state shall permanently revoke the electronic notary public's commission.

§ 41-368. Grounds for refusal, suspension or revocation of commission

A. The secretary of state may refuse to appoint any person as an electronic notary public or may suspend or revoke the commission of any electronic notary public for any of the following reasons:

1. Substantial and material misstatement or omission in the application for an electronic notary public commission that is submitted to the secretary of state.

2. Conviction of a felony unless restored to civil rights, or of a lesser offense involving moral turpitude or of a nature that is incompatible with the duties of an electronic notary public. A conviction after a plea of no contest is deemed to be a conviction for purposes of this paragraph.

3. Revocation, suspension, restriction or denial of a professional license if that action was for misconduct, dishonesty or any cause that substantially relates to the duties or responsibilities of an electronic notary public.

4. Failure to discharge fully and faithfully any of the duties or responsibilities required of an electronic notary public.

5. The use of false or misleading advertising in which the electronic notary public has represented that the electronic notary public has duties, rights or privileges that the electronic notary public does not possess by law.

6. Charging more than the fees authorized by statute or rule.

7. The commission of any act involving dishonesty, fraud or deceit with the intent to substantially benefit the electronic notary public or another person or to substantially injure another person.

8. Failure to complete the electronic acknowledgment or electronic jurat at the time the electronic notary's signature and seal are affixed to the document.

9. Failure to administer the oath or affirmation required at the time of performing an electronic jurat for an individual.

10. Execution of any electronic notarial certificate by the electronic notary public containing a statement known by the electronic notary public to be false.

11. The return for insufficient funds or any other reason for nonpayment of a check issued for fees to the secretary of state.

12. Notarizing a document that does not contain a notarial certificate.

B. If an application is denied, the secretary of state shall notify the applicant within thirty days after receipt of the application and shall state the reasons for the denial.

C. The secretary of state may suspend the commission of an electronic notary for at least thirty days and for not more than one hundred eighty days.

D. If a person has had an electronic notary commission in this state revoked, the secretary of state may refuse to appoint the person as an electronic notary for four years after the date of the revocation.

E. On revocation or suspension of an electronic notary public's commission, the secretary of state shall give notice to the electronic notary public and shall provide the person with notice of the opportunity for a hearing on the revocation or suspension pursuant to chapter 6, article 10 of this title.[7] The revocation or suspension of an electronic notary public commission is an appealable agency action.

§ 41-369. Duties of secretary of state

The secretary of state shall adopt rules pursuant to chapter 6 of this title[8] that establish policies, procedures, fees and any other duties or services required by this article.

§ 41-370. Complaints; investigations; failure to respond

A. Any person may make a complaint to the office of the secretary of state regarding an electronic notary. The secretary of state shall receive any complaints and shall provide notice of those complaints to the office of the attorney general. The office of attorney general shall investigate and take action on all complaints involving any allegation of a violation of this article.

B. An electronic notary's failure to respond to an investigation is a failure by the notary to fully and faithfully discharge the responsibilities and duties of an electronic notary.

Arizona Administrative Code R2-12-1201 through R2-12-1209

R2-12-1201. Application and Renewal

Each applicant for an electronic notary commission or a renewal of an electronic notary commission shall:

1. Submit to the Secretary of State a verified application on a form furnished by the Secretary of State that provides the following information about the applicant:
   a. Full name and any former names used by the applicant;
   b. Physical address and telephone number;
   c. Mailing address and telephone number;
   d. Business address, telephone number, fax number and email address, if applicable;
   e. County of residence;
   f. Gender;
   g. Date of birth;
   h. The previous commission number of the applicant if previously an electronic notary or notary public appointed under A.R.S. § 41-312 in Arizona, if applicable;
   i. Responses to questions regarding the applicant's background on the following subjects:

[7] Section 41-1092 et seq.
[8] Section 41-1001 et seq.

i. Whether the applicant has been convicted of a felony or an undesignated offense in this or any other jurisdiction and whether the applicant has been restored to civil rights.
ii. Whether the applicant has been convicted of a lesser offense involving moral turpitude or of a nature that is incompatible with the duties of a notary public in this or any other jurisdiction such as a finding that the applicant engaged in conduct that would violate A.R.S. § 41-313 if adjudicated in Arizona, or that the applicant engaged in conduct that constituted misconduct in public office or demonstrated dishonesty or a lack of veracity.
iii. Whether the applicant has ever had a professional license revoked, suspended, restricted, or denied for misconduct, dishonesty, or any cause that relates to the duties or responsibilities of a notary public such as a finding that the applicant engaged in conduct that would violate A.R.S. § 41-313 if adjudicated in Arizona, or that the applicant engaged in conduct that demonstrated dishonesty or a lack of veracity.
iv. Whether the applicant has had a notary commission revoked, suspended, restricted, or denied in this state or any other jurisdiction.
v. Statement that applicant is 18 years of age or older.
vi. Statement of being an Arizona resident.
vii. Whether the applicant holds or has held a notary commission in another state or jurisdiction and the commission number and jurisdiction, if applicable.

2. The Secretary of State may require that the applicant provide a detailed explanation and supporting docu-mentation for each response on the application regarding the applicant's background.
3. Each applicant shall register with the Secretary of State the applicant's possession of an approved electronic notary token within 90 days of submitting the application.

R2-12-1202. Applicant Filing Fee, Bond, and Bond Filing Fee

A. The application and renewal fee is $25.
B. The bond filing fee is $25.
C. The applicant shall purchase a surety bond in the amount of $25,000. The original bond shall be filed with the Secretary of State's office accompanying the application or renewal.
D. The bond shall contain, on its face, the oath of office for the electronic notary public as specified in A.R.S. § 38-231(G). The electronic notary shall endorse the oath on the face of the bond, immediately below the oath, by signing the electronic notary's name under which the person has applied to be commissioned as an electronic notary and exactly as the name appears on the electronic notary application form filed with the Secretary of State's Office.

R2-12-1203. Notarial Journal

A. An electronic notary public shall keep a journal of all electronic notarial acts in bound paper form with the same form as required in A.R.S. § 41-319 herein referenced as a "journal." If an electronic notary act is conducted upon an electronic signature that is not recognized under A.R.S. § 41-132, the electronic notary shall have the signer sign the paper journal in a manner consistent with A.R.S. § 41-319.
B. The journal shall be under the control of the electronic notary.

C. If an electronic notary also holds commission as a notary public appointed under A.R.S. § 41-312, and the commission dates are identical between the two commissions, then the electronic notary may use the notary public journal as the electronic notary paper journal. If the dates are not identical, then the electronic notary shall maintain two separate journals.

D. If a notary service electronic certificate is used in a manner to create an electronic signature in a notarial act, the document name, title, brief description of contents, and the time stamp shall be entered into the issuing electronic notary's journal as a notary service electronic certificate entry.

E. Journals are not deemed received until the Secretary of State accepts the journals as complete. The electronic notary shall not be subject to a penalty for delay outside the control of the electronic notary in delivering the journal to the Secretary of State.

R2-12-1204. Standards for Electronic Notary Token and Notary Service Electronic Certificate

A. An electronic notary token, and subsequently a notary service electronic certificate, shall be approved under A.R.S. § 41-132.

B. A provider of an electronic notary token may not provide an official electronic notary token to a person unless the person first presents evidence of the electronic notary commission for that person to the provider.

C. A provider of a notary service electronic certificate may not provide an official notary service electronic certificate to a person unless the person presents himself or herself before and receives authorization from an electronic notary for reception of the notary service electronic certificate.

D. An electronic notary token shall contain:

1. The commission number of the electronic notary;
2. The full name of the electronic notary, as commissioned as an electronic notary;
3. The expiration date of the notary's commission;
4. A link to the commission record of the electronic notary on the Secretary of State's official web site; and
5. Any applicable information relative to A.R.S. § 41-132.

E. A notary service electronic certificate shall contain:

1. The commission number of the electronic notary authorizing the notary service electronic certificate;
2. The identification of the authorizing electronic notary's electronic notary token;
3. The full name of the individual, as presented to the electronic notary;
4. A link to the authorizing commission record of the electronic notary on the Secretary of State's official web site; and
5. Any applicable information relative to A.R.S. § 41-132.

F. An electronic notary may possess only one electronic notary token.

R2-12-1205. Use of Electronic Notary Tokens and Notary Service Electronic Certificate

A. An electronic notary may only use an electronic notary token for the duties set forth in A.R.S. §§ 41-351 through 41-369 and interactions with the provider of the electronic notary token.

B. A person may only use a notary service electronic certificate for the purposes of creating electronic notarized documents and interactions with the provider of the notary service electronic certificate.

C. Use of an electronic notary token is not complete without:

1. Incorporating the electronic notary token elements into the document;
2. Either directly incorporating the time and date of notarization or incorporating the time and date of notarization using a process of an approved time stamp provider;
3. Affixing the notary's electronic signature.

D. Use of a notary service electronic certificate is not complete without:

1. Presence of a date and time stamp from an approved time stamp token provider;
2. Affixing the notary's electronic signature.

R2-12-1206. Approval of Time Stamp Token Provider

Any person or entity that can provide a service that synchronizes time as defined in A.R.S. § 1-242 into a process using an electronic notary token or a notary service electronic certificate, where applicable, may be added to the list of approved time stamp token providers. All time stamp tokens that interact with electronic notary tokens and notary service electronic certificates need to meet the applicable technology standards required by A.R.S. § 41-132.

R2-12-1207. Fees

Electronic notaries may charge the following fees:

1. Fee for an acknowledgment shall be not more than $25.
2. Fee for an oath or affirmation shall be not more than $25.
3. Fee for a jurat shall be not more than $25.
4. Fee for authorizing a notary service electronic certificate to a person shall be not more than $50. This does not include any vendor fees or charges to the person for reception of the notary service electronic certificate.
5. Fee for any other notarial act shall be not more than $25.

R2-12-1208. Penalty Fee for Lack of Notice

The penalty to be imposed upon an electronic notary for failure to provide signed notice as defined in the statute to the Secretary of State of each loss, theft, or compromise of the electronic notary's journal shall be $10 per use of electronic notary token up to a maximum of $500. When audit trail is not recoverable, the maximum of $500 shall be imposed upon the electronic notary for each failure to provide proper notice of a loss, theft, or compromise of the electronic notary's journal.

R2-12-1209. Civil Penalties

A. The penalty to be imposed upon an electronic notary for failure to provide signed notice as defined in the statute to the Secretary of State of each loss, theft, or compromise of a notary service electronic certificate or of loss, theft or compromise of any materials or processes used in creating an electronic notary token or authorizing a notary service electronic certificate shall be $10 per day, up to a maximum of $500 for each failure to provide proper notice of a loss, theft, or compromise of a notary service electronic certificate or compromise of any materials or processes used in creating an electronic notary token.

B. The penalty to be imposed upon an electronic notary for each failure to provide signed notice as defined in the statute to the Secretary of State of a change of address shall be $10 per day, up to a maximum of $250 for each failure to provide proper notice of a change of address.

C. The penalty to be imposed upon an electronic notary for failure to deposit the notary's electronic notary journal and records as defined in the statute with the Secretary of State shall be $50 for the first day and then $10 per day up to a maximum of $500.

Appendix E
PRIA Standards and Guidelines

The most current version of the following PRIA standards and guidelines may be found at: http://www.pria.us. Prior to accessing the documents listed below, the user will be required to agree to the terms and conditions of the PRIA eRecording XML Standards License Agreement that may be found at: http://www.pria.us/Papers/licensedpapers/dtd.htm.

Technical Standards

- Document Version 2.4.1 September 2006
- Notary Version 2.4.1 September 2006
- PRIA Request Version 2.4.1 September 2006
- PRIA Response Version 2.4.1 September 2006

Guidelines

- PRIA URPERA Enactment and eRecording Standards Implementation Guide
- PRIA eRecording XML Implementation Guide (Technical iGuide)

Appendix F
Records Retention and Preservation Statutes

For the most recent version of the statutes, please click on the hyperlink.

Arizona State Library, Archives and Public Records

§ 41-1330. Definitions

In this article, unless the context otherwise requires:

1. "Board" means the board of the state library.

2. "Director" means the director of the state library.

3. "State library" means the Arizona state library, archives and public records.

§ 41-1331. Arizona state library, archives and public records

A. The Arizona state library, archives and public records is established in the legislative branch of state government.

B. The state library shall:

1. Acquire and provide access to materials relating to the following in print, in an electronic format or in any other format:

(a) Law.

(b) Political science.

(c) Economics.

(d) Sociology.

(e) Subjects pertaining to the theory and practice of government.

(f) Genealogy.

(g) Arizona history.

2. Provide the following:

(a) A general and legal reference service.

(b) A records management and archives program.

(c) A state and federal government documents depository program.

(d) A library development service.

(e) Museums for educational purposes as approved by the board.

(f) A service, including materials, for persons who are visually or physically unable to use traditional print materials.

§ 41-1332. Board of the Arizona state library, archives and public records; appointment of director

A. A board of the Arizona state library, archives and public records is established consisting of the president of the senate, speaker of the house of representatives, one member of the senate appointed by the president of the senate and one member of the house of representatives appointed by the speaker of the house of representatives.

B. Meetings of the board shall be held at the call of the chairman. The speaker of the house of representatives shall serve as chairman in even-numbered years and the president of the senate shall serve as chairman in odd-numbered years.

C. The board shall exercise general supervision over the state library and shall appoint the director of the state library. The director shall serve at the pleasure of the board.

§ 41-1333. Director of the state library; qualifications

A. The state library shall be under the charge and control of a director, subject to board supervision.

B. The director shall be a person technically trained in library work or have at least five years' actual experience as chief administrator of a major library.

§ 41-1334. Compensation of director

The compensation of the director shall be as determined by the board.

§ 41-1335. Powers and duties of director

A. The director shall:

1. Adopt rules for the use of books or other materials in the custody of the state library and for the removal of books from the library, including assessment of reasonable penalties for failure to return books or other materials when due. The proceeds from the assessment of reasonable penalties shall be deposited, pursuant to §§ 35-146 and 35-147, in the state library fund

established by § 41-1336. The monies shall be used only for the purchase of other books or materials.

2. Sell or exchange undesired duplicate copies of books or other materials, or books or other materials not of value for the purposes of the library, or photographic reproductions of state library holdings, and deposit, pursuant to §§ 35-146and 35-147, the proceeds in the state library fund established by § 41-1336. The monies shall be used for the purchase of other books or materials.

3. Bring actions for the recovery of books, or for three times the value of the books, against any person who has them in the person's possession or who is responsible for the books, and who has failed or refused to return them on demand. If a book is one of a set the value of the book may be deemed the value of the entire set. Monies recovered pursuant to this paragraph shall be transmitted to the state treasurer for credit to the state library fund established by § 41-1336.

4. Certify copies from books, documents or other archival or public records which have been deposited in the custody of the state library. The fee for certification shall be the same as prescribed for the certification of records by the secretary of state. These fees shall be transmitted to the state treasurer for credit to the state library fund established by § 41-1336. These certificates have the same force and effect as if made by the officer originally in charge of the record.

5. As the director deems necessary:

(a) Arrange with the federal government, other states and foreign countries for a system of exchange of official state reports and publications, session laws, statutes, legislative journals and supreme court reports.

(b) Enter into agreements to establish a depository system and an exchange program with any municipal, county or regional public library, state college or state university library and out-of-state research libraries.

(c) Enter into agreements with libraries in this state for the state documents program described in § 41-1338, subsection A, paragraph 2. Any library that enters into an agreement pursuant to this subdivision shall continue to contribute at least the same level of support to the state documents program and shall not use any monies received pursuant to the agreement to supplant other monies available to the library.

6. Adopt rules for the acquisition, maintenance, access and preservation of state publications.

7. After consultation with other appropriate agencies, adopt rules for the description of state publications in all formats.

8. Provide access to an official compilation or revision of the laws of this state to each public or court library in this state that applies for access. The director may provide the access

electronically. On request, the director may provide a certified copy of a law pursuant to paragraph 4 of this subsection.

9. Annually submit a report to the legislature on the condition of the state library, its activities and the disposition of monies spent for its maintenance and transmit a copy of the report to the governor.

10. Appoint personnel, including security personnel, necessary to perform the duties of the state library and assign their duties.

11. Cooperate with the legislative council in carrying out § 41-1304, subsection B.

B. The governor, the secretary of state, the president of the senate, the speaker of the house of representatives, the heads of departments and all officers and agents of this state shall supply at no cost the number of copies of official reports, public documents and publications required for the state library or its agents to satisfy the requirements of the state documents program or arrangements or agreements entered into pursuant to subsection A, paragraph 5 of this section.

C. The governmental units described in subsection B of this section shall:

1. Notify the state library if the reports, documents and publications subject to this section are posted on an internet web site.

2. Pay the state library the fee charged pursuant to § 41-1345 if the governmental unit refuses the state library's request to supply, and the state library incurs any expenses in obtaining, the copies that are required to be supplied pursuant to this section.

§ 41-1336. State library administrative agency; state library fund

A. The state library is the state library administrative agency, and the director may accept, on behalf of the state, any allocation of money or materials made by the federal government for state library purposes, any appropriations of state monies for the purposes of this article or any bequests, grants or gifts to the state library, and administer all of them under rules adopted by the director, unless otherwise provided by law. The administration shall not be inconsistent with the conditions of the allocation, appropriation, bequest, grant or gift.

B. A state library fund is established. All monies received pursuant to this section and § 41-1335, except for federal monies, shall be deposited, pursuant to §§ 35-146 and 35-147, in the fund and accounted for separately. Monies in the accounts are continuously appropriated to the state library for the purposes provided for in the fund sources, and monies in the fund are exempt from the provisions of § 35-190 relating to lapsing of appropriations. On notice from the director, the state treasurer shall invest and divest monies in the fund as provided by § 35-313, and monies earned from investment shall be credited to the fund.

C. All federal monies received as provided by this section shall be deposited, pursuant to §§ 35-146 and 35-147, in a separate account of the fund and disbursed in the manner prescribed for the disbursement of state funds, but shall not be subject to § 35-190 relating to lapsing appropriations.

§ 41-1337. Library development service

The state library shall:

1. Prepare a plan for statewide public library service. The plan shall be put into effect to the extent made practicable by available facilities.

2. Encourage and assist the development of library services in state institutions.

3. Compile and disseminate statistics and other data relating to libraries and library services.

4. Give professional advice and assistance in the establishment and operation of county free libraries, municipal libraries, or any combinations of county free and municipal libraries, and to joint ventures of public and private or nonprofit libraries in this state that make library information available to the public and that request such professional advice and assistance.

5. Develop library service for the blind and physically disabled, including talking book machine services, through state and regional centers.

6. Perform all other duties necessary or appropriate to the development of statewide library service.

§ 41-1338. Archives and history services; recovery of costs

A. The state library shall contain:

1. All available works, books, newspaper files, pamphlets, papers, manuscripts, documents, magazines and newspaper articles, maps, pictures, items and materials pertaining to or bearing on the history of Arizona.

2. Copies of current official reports, public documents and publications of state, county and municipal officers, departments, boards, commissions, agencies and institutions, and public archives. To permit compliance with this paragraph it is the duty of all public officers required by law to make written reports to the governor, or to the governing officer or body of a county, city or town, to provide those reports, documents and publications to the state library for filing in the state library archives in the number that will satisfy the requirements of the state documents program or arrangements or agreements entered into pursuant to § 41-1335, subsection A, paragraph 5 except those reports, documents and publications that are confidential.

B. The governmental units described in subsection A of this section shall:

1. Notify the state library if the reports, documents and publications subject to this section are posted on an internet web site.

2. Pay the state library the fee charged pursuant to § 41-1345 if the governmental unit refuses the state library's request to provide, and the state library incurs any expenses in obtaining, the copies that are required to be provided pursuant to this section.

§ 41-1339. Depository of official archives

A. The state library is the central depository of all official books, records and documents not in current use of the various state officers and departments of the state, the counties and incorporated cities and towns. These materials constitute the state archives. The state archives shall be carefully kept and preserved, classified, catalogued and made available for inspection under rules the director adopts.

B. State officers in possession of official state or territorial archives shall deposit those archives with the state library.

C. Any county, municipal or other public official may either retain or deposit with the state library for permanent preservation official books, records, documents and original papers not in current use. The clerk of the superior court shall deposit and the state archives shall preserve all permanent superior court case files pursuant to court rules.

D. The state library shall make birth and death records held in the state library archives available for inspection as follows:

1. Birth records if seventy-five years have passed after the date of birth as recorded on the birth certificate.

2. Death records if fifty years have passed after the date of death.

§ 41-1340. Historical records

The state library shall:

1. Collect from the files of old newspapers, court records, church records, private collections and other sources, data pertaining to the history of the state.

2. Accept loans or gifts of rare volumes, manuscripts, maps, pictures and other articles or things of historical value.

3. Classify, edit, annotate and publish from time to time records considered of public interest.

4. Encourage the proper marking of points of historical importance.

5. Systematically stimulate historical research and encourage the study of Arizona history.

§ 41-1343. Access to public records

The director, in person or through a deputy, has the right of reasonable access to all nonconfidential public records in the state, or any public office of the state or any county, city, municipality, district or political subdivision of the state, because of the historical and research value of data contained in those records, with a view to securing their safety and determining their need for preservation or disposal.

§ 41-1345. Records; records management; powers and duties of director; fees; records services fund

A. The director is responsible for the preservation and management of records. In addition to other powers and duties, the director shall:

1. Establish standards, procedures and techniques for effective management of records.

2. Make continuing surveys of record keeping operations and recommend improvements in current record management practices including the use of space, equipment and supplies employed in creating, maintaining, storing and servicing records.

3. Establish standards and procedures for the preparation of schedules providing for the retention of records of continuing value and for the prompt and orderly disposal of records no longer possessing sufficient administrative, legal or fiscal value to warrant their further keeping.

4. Establish criteria for designation of essential records within the following general categories:

(a) Records containing information necessary to the operations of government in the emergency created by a disaster.

(b) Records containing information necessary to protect the rights and interests of persons or to establish and affirm the powers and duties of governments in the resumption of operations after a disaster.

5. Reproduce or cause to be reproduced essential records and prescribe the place and manner of their safekeeping.

6. Obtain such reports and documentation from agencies as are required for the administration of this program.

7. Request transmittal of the originals of records produced or reproduced by agencies of the state or its political subdivisions pursuant to § 41-1348 or certified negatives, films or electronic media of such originals, or both, if in the director's judgment such records may be of historical or other value.

8. On request, assist and advise in the establishment of records management programs in the legislative and judicial branches of the state and provide program services similar to those available to the executive branch of state government pursuant to this article.

9. Establish a fee schedule to systematically charge state agencies, political subdivisions of this state and other governmental units of this state for services described in this section and § 41-1345.01 and deposit monies received from fees in the records services fund established by subsection B of this section.

10. Subject to approval of the board, establish a fee schedule to charge state agencies, political subdivisions of this state and other governmental units of this state for services and expenses incurred by the state library in obtaining copies of those reports, documents and publications that are required to be delivered, supplied or provided pursuant to §§ 35-103, 41-1335 and 41-1338 and deposit these monies in the records services fund established by subsection B of this section.

B. A records services fund is established consisting of monies deposited pursuant to subsection A, paragraphs 9 and 10 of this section. The director shall administer the fund for the purposes provided in subsection A of this section. Monies in the fund are subject to legislative appropriation and are exempt from the provisions of § 35-190 relating to lapsing of appropriations.

§ 41-1345.01. Records management officer; duties

A. The state library shall employ a records management officer who is responsible for the direction and control of the records management program. The records management officer shall at the direction of the director administer the provisions of § 41-1345.

B. The state library shall:

1. Through consultation and education, provide for an efficient and contemporary records management program using modern techniques to facilitate the efficient and economic creation, maintenance, control, retention and disposition of records as defined in § 41-1350.

2. Operate a records management center for the maintenance and housing of inactive non-archival records. The records management center shall be the only inactive records center operated by a state agency. State agencies may use other facilities for inactive records storage with prior approval of the director.

3. Establish standards and procedures for records accepted for storage.

4. Operate a secure vault as part of the records management center for the housing and maintenance of micrographic, machine read and selected essential records.

5. Operate a preservation imaging function that is responsible for:

(a) The efficient and coordinated use of micrographics and digital imaging equipment,

techniques and personnel to achieve optimum quality, effectiveness and economy in the production of source document micrographics and digital imaging.

(b) The processing and duplication of microfilm produced by the preservation imaging operation and film produced by other agencies of this state.

§ 41-1346. State and local public records management; violation; classification; definition

A. The head of each state and local agency shall:

1. Establish and maintain an active, continuing program for the economical and efficient management of the public records of the agency.

2. Make and maintain records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures and essential transactions of the agency designed to furnish information to protect the rights of the state and of persons directly affected by the agency's activities.

3. Submit to the director, in accordance with established standards, schedules proposing the length of time each record series warrants retention for administrative, legal or fiscal purposes after it has been received by the agency.

4. Submit a list of public records in the agency's custody that are not needed in the transaction of current business and that are not considered to have sufficient administrative, legal or fiscal value to warrant their inclusion in established disposal schedules.

5. Submit to the director lists of all essential public records in the custody of the agency.

6. Cooperate with the director in the conduct of surveys.

7. Designate an individual within the agency to manage the records management program of the agency. The designated individual:

(a) Must be at a level of management sufficient to direct the records management program in an efficient and effective manner.

(b) Shall act as coordinator and liaison for the agency with the state library.

8. Comply with rules, standards and procedures adopted by the director.

B. The governing body of each county, city, town or other political subdivision shall promote the principles of efficient record management for local public records. Such governing body shall, as far as practicable, follow the program established for the management of state records. The director shall, upon request of the governing body, provide advice and assistance in the establishment of a local public records management program.

C. A head of a state or local agency who violates this section is guilty of a class 2 misdemeanor.

D. For the purposes of this section, "records management" means the creation and implementation of systematic controls for records and information activities from the point where they are created or received through final disposition or archival retention, including distribution, use, storage, retrieval, protection and preservation.

§ 41-1347. Preservation of public records

A. All records made or received by public officials or employees of this state in the course of their public duties are the property of the state. Except as provided in this article, the director and every other custodian of public records shall carefully protect and preserve the records from deterioration, mutilation, loss or destruction and, when advisable, shall cause them to be properly repaired and renovated. All paper, ink and other materials used in public offices for the purpose of permanent records shall be of durable quality and shall comply with the standards established pursuant to § 39-101.

B. Records shall not be destroyed or otherwise disposed of by any agency of the state, unless it is determined by the state library that the record has no further administrative, legal, fiscal, research or historical value. The original of any record produced or reproduced pursuant to § 41-1348 may be determined by the state library to have no further administrative, legal, fiscal, research or historical value. A person who destroys or otherwise disposes of records without the specific authority of the state library is in violation of § 38-421.

§ 41-1348. Production and reproduction of records by agencies of the state and political subdivisions; admissibility; violation; classification

A. Each agency of the state or any of its political subdivisions may implement a program for the production or reproduction by photography or other method of reproduction on film or electronic media of records in its custody, whether obsolete or current, and classify, catalogue and index such records for convenient reference. The agency, prior to the institution of any such program of production or reproduction, shall obtain approval from the director of the types of records to be produced or reproduced and of the methods of production, reproduction and storage and the equipment which the agency proposes to use in connection with the production, reproduction and storage.

B. Except as otherwise provided by law, records reproduced as provided in subsection A of this section are admissible in evidence.

C. The provisions of this section shall not be applicable to permit destruction of current original affidavits of registration as that term is used in § 16-163.

D. A head of an agency of this state or a political subdivision of this state who violates this section is guilty of a class 2 misdemeanor.

§ 41-1349. Duties relating to historical value

A. The state library shall:

1. Determine whether public records presented to it are of historical value.

2. Dispose of records determined to be of no historical value.

3. Accept those records deemed by a public officer having custody of the records to be unnecessary for the transaction of the business of the public officer's office and deemed to be of historical value.

B. All public records of any public office, upon the termination of the existence and functions of the office, shall be checked by the state library and either disposed of or transferred to the custody of the state library, in accordance with this article. If a public office is terminated or reduced by the transfer of its powers and duties to another office or to other offices, its appropriate public records shall pass with the powers and duties transferred.

§ 41-1350. Definition of records

In this chapter, unless the context otherwise requires, "records" means all books, papers, maps, photographs or other documentary materials, regardless of physical form or characteristics, including prints or copies of such items produced or reproduced on film or electronic media pursuant to § 41-1348, made or received by any governmental agency in pursuance of law or in connection with the transaction of public business and preserved or appropriate for preservation by the agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the government, or because of the informational and historical value of data contained therein. Library or museum material made or acquired solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference and stocks of publications or documents intended for sale or distribution to interested persons are not included within the definition of records as used in this chapter.

§ 41-1351. Determination of value; disposition

Every public officer who has public records in the public officer's custody shall consult periodically with the state library and the state library shall determine whether the records in question are of legal, administrative, historical or other value. Those records determined to be of legal, administrative, historical or other value shall be preserved. Those records determined to be of no legal, administrative, historical or other value shall be disposed of by such method as the state library may specify. A report of records destruction that includes a list of all records disposed of shall be filed at least annually with the state library on a form prescribed by the state library.

§ 41-1352. Historical advisory commission; membership; terms; expenses; duties; historic sites review committee

A. A historical advisory commission is established consisting of members appointed by the director for staggered terms of three years ending on July 1. The commission membership of not less than ten nor more than twenty members shall consist of experts in the disciplines of history, arts and culture, architecture and archaeology, professional librarians and archivists or persons otherwise associated with the interpretation, research, writing, preservation or teaching of this state's heritage, including the Indian nations' history and heritage, and the director of the Arizona historical society, the director of the state museum, the director of the Arizona state parks board and the state historic preservation officer.

B. Members shall serve without compensation but those employed by the state shall be reimbursed for travel and subsistence by the department or agency they represent and those who are not employed by the state are eligible for reimbursement of expenses by the commission pursuant to title 38, chapter 4, article 2.[9]

C. The commission shall:

1. Advise the legislature and state agencies on matters relating to this state's history and historic preservation.

2. Recommend measures to the legislature and state agencies to coordinate or improve the effectiveness of activities of state agencies and agencies of the political subdivisions of this state and other persons relating to the interpretation, research, writing and teaching of this state's history, heritage and historic preservation, including the Indian nations' history, heritage and preservation.

3. Advise the legislature and state agencies on the dissemination of information pertaining to activities relating to historic preservation as provided in paragraph 2.

4. Encourage, in cooperation with appropriate public and private agencies, the Indian nations and other persons, training and education in the field of the interpretation, research, writing and teaching of this state's history, heritage and historic preservation.

5. Submit annually on September 30 a report of the commission's activities to the director for inclusion in the annual report of the state library.

D. A historic sites review committee consisting of nine members is established to serve as a standing committee of the historical advisory commission. The state historic preservation officer shall appoint committee members for staggered terms of three years ending on July 1. The state historic preservation officer may appoint persons other than commission members to serve on the committee and shall appoint at least five persons who are professionals qualified in the disciplines of history, prehistoric and historic archaeology, architectural history or architecture.

[9] Section 38-621 et seq.

The committee shall select annually at the first meeting a chairman who is a commission member. The chairman shall report on committee activities at commission meetings. The committee shall assist in the duties prescribed in this section and by federal law, review nominations to the national and state historic registers, provide general advice and guidance to the state historic preservation officer and perform other duties as are necessary. On or before September 1 of each year, the state historic preservation officer shall submit a report of the committee's activities to the governor, the president of the senate, the speaker of the house of representatives and the director, including information prescribed in §§ 41-862 and 41-881.

§ 41-1353. Review and transfer of certain historic property; exemption; definition

A. An agency shall notify the state library on forms prescribed by the director if the agency has or acquires furniture, equipment or other personal property which is fifty or more years of age or of known historical interest, including property escheated to the state under title 12, chapter 7, article 5.[10]

B. The director may authorize a person to inspect the personal property reported under subsection A and recommend to the state library whether the personal property is of an historic interest or value as would in the public interest require it to be made available permanently for placement on public display in any restored executive, legislative or judicial facility or museum area.

C. If the state library determines the personal property should be made available for display purposes it shall provide written notice to the agency requesting prompt transfer of the personal property to the state library.

D. An agency may apply to the board for an exemption from the transfer required under subsection C by filing a prompt written response to the board stating:

1. The length of time the agency has used the personal property.

2. Why the value of the personal property to the agency is greater than the educational and historic value in displaying the personal property.

3. What harm the agency would suffer if the personal property is transferred to the department.

4. That the use of federal monies in the initial acquisition of the personal property legally precludes its transfer to the board.

E. The board shall grant an exemption to a requested property transfer if it finds that the transfer of the property would result in significant cost or disruption to the agency which would outweigh the educational and historic value in displaying the property.

[10] Section 12-881 et seq.

F. For the purposes of this section, "agency" means any branch, department, commission, board or other unit of the state organization which receives, disburses or expends state monies or incurs obligations against this state.

§ 41-1354. Privacy of user records; exceptions; violation; classification

A. Except as provided in subsection B, a library or library system supported by public monies shall not allow disclosure of any record or other information which identifies a user of library services as requesting or obtaining specific materials or services or as otherwise using the library.

B. Records may be disclosed:

1. If necessary for the reasonable operation of the library.

2. On written consent of the user.

3. On receipt of a court order.

4. If required by law.

C. Any person who knowingly discloses any record or other information in violation of this section is guilty of a class 3 misdemeanor.

§ 41-1355. Arizona historical records advisory board

A. An Arizona historical records advisory board is established consisting of the director and At least six members appointed by the director. These members shall consist of recognized experts in the administration of government records, historical records or archives and shall be as broadly representative as possible of public and private archives, records offices and research institutions and organizations in this state.

B. Members appointed by the director pursuant to subsection A shall serve three year staggered terms beginning on July 1. If there is a vacancy, the director shall appoint another person to serve the remainder of the term. The director may appoint members to succeeding terms. The director may remove a member for good and sufficient cause.

C. The advisory board shall annually elect a chairperson and vice-chairperson from among its members at the first meeting of the fiscal year. The director shall serve as secretary of the advisory board and shall maintain the records of the advisory board.

D. The director shall call quarterly meetings and the director or chairperson may call other meetings as the director or chairperson deems necessary. A member of the advisory board may send a designee to be an observer at advisory board meetings. the designee may not vote directly or as a proxy.

E. The advisory board shall:

1. Serve as the central advisory body for historical records planning and for national historical publications and records commission funded projects developed and carried out in this state.

2. Serve as a coordinating body to facilitate cooperation among historical records repositories and other information agencies in this state and as a state-level review body for grant proposals as defined in the national historical publications and records commission guidelines.

F. The advisory board may:

1. Sponsor and publish surveys of the conditions and needs of historical records in this state.

2. Solicit or develop proposals for projects to be carried out in this state with national historical publications and records commission grants.

3. Review proposals by institutions in this state and make recommendations about these proposals to the national historical publications and records commission.

4. Develop, revise and submit to the national historical publications and records commission this state's priorities for historical records projects according to guidelines developed by the national historical publications and records commission.

5. Promote an understanding of the role and value of historical records.

6. Act in an advisory capacity to the state archives and other statewide archival or records agencies.

7. Review, through reports and otherwise, the operation and progress of projects in this state that are financed by national historical publications and records commission grants.

G. Members of the advisory board are not eligible to receive compensation but are eligible for reimbursement of expenses pursuant to title 38, chapter 4, article 2.[11]

[11] Section 38-621 et seq.

Arizona Public Records Law

Article 1. Requirements for Material Used

§ 39-101. Permanent public records; quality; storage; violation; classification

A. Permanent public records of the state, a county, city or town, or other political subdivision of the state, shall be transcribed or kept on paper or other material which is of durable or permanent quality and which conforms to standards established by the director of the Arizona state library, archives and public records.

B. Permanent public records transcribed or kept as provided in subsection A shall be stored and maintained according to standards for the storage of permanent public records established by the director of the Arizona state library, archives and public records.

C. A public officer charged with transcribing or keeping such public records who violates this section is guilty of a class 2 misdemeanor.

§ 39-102. Annual report; copies

Unless otherwise specifically required by law, each agency, board, commission and department which prepares an annual report of its activities shall prepare and distribute as provided by law copies of such annual report on twenty pound bond paper printed with black ink except that the cover and back pages may be of sixty-five pound or less cover paper.

§ 39-103. Size of public records; exemptions

A. All public records of this state or a political subdivision of this state created on paper, regardless of weight or composition, shall conform to standard letter size of eight and one-half inches by eleven inches, within standard paper manufacturing tolerances.

B. This section does not apply to public records smaller than eight and one-half inches by eleven inches, public records otherwise required by law to be of a different size, engineering drawings, architectural drawings, maps, computer generated printout, output from test measurement and diagnostic equipment, machine generated paper tapes and public records otherwise exempt by law. Upon written application the director of the Arizona state library, archives and public records may approve additional exemptions from this section if based upon such application the director finds that the cost of producing a particular type of public record in accordance with subsection A is so great as to not be in the best interests of this state.

Article 2. Searches and Copies

§ 39-121. Inspection of public records

Public records and other matters in the custody of any officer shall be open to inspection by any person at all times during office hours.

§ 39-121.01. Definitions; maintenance of records; copies, printouts or photographs of public records; examination by mail; index

A. In this article, unless the context otherwise requires:

1. "Officer" means any person elected or appointed to hold any elective or appointive office of any public body and any chief administrative officer, head, director, superintendent or chairman of any public body.

2. "Public body" means the state, any county, city, town, school district, political subdivision or tax-supported district in the state, any branch, department, board, bureau, commission, council or committee of the foregoing, and any public organization or agency, supported in whole or in part by monies from the state or any political subdivision of the state, or expending monies provided by the state or any political subdivision of the state.

B. All officers and public bodies shall maintain all records, including records as defined in § 41-1350, reasonably necessary or appropriate to maintain an accurate knowledge of their official activities and of any of their activities which are supported by monies from the state or any political subdivision of the state.

C. Each public body shall be responsible for the preservation, maintenance and care of that body's public records, and each officer shall be responsible for the preservation, maintenance and care of that officer's public records. It shall be the duty of each such body to carefully secure, protect and preserve public records from deterioration, mutilation, loss or destruction, unless disposed of pursuant to §§ 41-1347 and 41-1351.

D. Subject to § 39-121.03:

1. Any person may request to examine or be furnished copies, printouts or photographs of any public record during regular office hours or may request that the custodian mail a copy of any public record not otherwise available on the public body's web site to the requesting person. The custodian may require any person requesting that the custodian mail a copy of any public record to pay in advance for any copying and postage charges. The custodian of such records shall promptly furnish such copies, printouts or photographs and may charge a fee if the facilities are available, except that public records for purposes listed in § 39-122 or 39-127 shall be furnished without charge.

2. If requested, the custodian of the records of an agency shall also furnish an index of records or categories of records that have been withheld and the reasons the records or categories of records have been withheld from the requesting person. The custodian shall not include in the index information that is expressly made privileged or confidential in statute or a court order. This paragraph shall not be construed by an administrative tribunal or a court of competent jurisdiction to prevent or require an order compelling a public body other than an agency to furnish an index. For the purposes of this paragraph, "agency" has the same meaning prescribed

in § 41-1001, but does not include the department of public safety, the department of transportation motor vehicle division, the department of juvenile corrections and the state department of corrections.

3. If the custodian of a public record does not have facilities for making copies, printouts or photographs of a public record which a person has a right to inspect, such person shall be granted access to the public record for the purpose of making copies, printouts or photographs. The copies, printouts or photographs shall be made while the public record is in the possession, custody and control of the custodian of the public record and shall be subject to the supervision of such custodian.

E. Access to a public record is deemed denied if a custodian fails to promptly respond to a request for production of a public record or fails to provide to the requesting person an index of any record or categories of records that are withheld from production pursuant to subsection D, paragraph 2 of this section.

§ 39-121.02. Action on denial of access; costs and attorney fees; damages

A. Any person who has requested to examine or copy public records pursuant to this article, and who has been denied access to or the right to copy such records, may appeal the denial through a special action in the superior court, pursuant to the rules of procedure for special actions against the officer or public body.

B. The court may award attorney fees and other legal costs that are reasonably incurred in any action under this article if the person seeking public records has substantially prevailed. Nothing in this paragraph[12] shall limit the rights of any party to recover attorney fees pursuant to § 12-341.01, subsection C, or attorney fees, expenses and double damages pursuant to § 12-349.

C. Any person who is wrongfully denied access to public records pursuant to this article has a cause of action against the officer or public body for any damages resulting from the denial.

§ 39-121.03. Request for copies, printouts or photographs; statement of purpose; commercial purpose as abuse of public record; determination by governor; civil penalty; definition

A. When a person requests copies, printouts or photographs of public records for a commercial purpose, the person shall provide a statement setting forth the commercial purpose for which the copies, printouts or photographs will be used. Upon being furnished the statement the custodian of such records may furnish reproductions, the charge for which shall include the following:

1. A portion of the cost to the public body for obtaining the original or copies of the documents, printouts or photographs.

[12] So in original. Probably should read "subsection".

2. A reasonable fee for the cost of time, materials, equipment and personnel in producing such reproduction.

3. The value of the reproduction on the commercial market as best determined by the public body.

B. If the custodian of a public record determines that the commercial purpose stated in the statement is a misuse of public records or is an abuse of the right to receive public records, the custodian may apply to the governor requesting that the governor by executive order prohibit the furnishing of copies, printouts or photographs for such commercial purpose. The governor, upon application from a custodian of public records, shall determine whether the commercial purpose is a misuse or an abuse of the public record. If the governor determines that the public record shall not be provided for such commercial purpose the governor shall issue an executive order prohibiting the providing of such public records for such commercial purpose. If no order is issued within thirty days of the date of application, the custodian of public records shall provide such copies, printouts or photographs upon being paid the fee determined pursuant to subsection A.

C. A person who obtains a public record for a commercial purpose without indicating the commercial purpose or who obtains a public record for a noncommercial purpose and uses or knowingly allows the use of such public record for a commercial purpose or who obtains a public record for a commercial purpose and uses or knowingly allows the use of such public record for a different commercial purpose or who obtains a public record from anyone other than the custodian of such records and uses it for a commercial purpose shall in addition to other penalties be liable to the state or the political subdivision from which the public record was obtained for damages in the amount of three times the amount which would have been charged for the public record had the commercial purpose been stated plus costs and reasonable attorney fees or shall be liable to the state or the political subdivision for the amount of three times the actual damages if it can be shown that the public record would not have been provided had the commercial purpose of actual use been stated at the time of obtaining the records.

D. For the purposes of this section, "commercial purpose" means the use of a public record for the purpose of sale or resale or for the purpose of producing a document containing all or part of the copy, printout or photograph for sale or the obtaining of names and addresses from public records for the purpose of solicitation or the sale of names and addresses to another for the purpose of solicitation or for any purpose in which the purchaser can reasonably anticipate the receipt of monetary gain from the direct or indirect use of the public record. Commercial purpose does not mean the use of a public record as evidence or as research for evidence in an action in any judicial or quasi-judicial body.

§ 39-122. Free searches for and copies of public records to be used in claims against United States; liability for noncompliance

A. No state, county or city, or any officer or board thereof shall demand or receive a fee or compensation for issuing certified copies of public records or for making search for them, when

they are to be used in connection with a claim for a pension, allotment, allowance, compensation, insurance or other benefits which is to be presented to the United States or a bureau or department thereof.

B. Notaries public shall not charge for an acknowledgment to a document which is to be so filed or presented.

C. The services specified in subsections A and B shall be rendered on request of an official of the United States, a claimant, his guardian or attorney. For each failure or refusal so to do, the officer so failing shall be liable on his official bond.

§ 39-123. Information identifying a peace officer, justice, judge, commissioner, public defender, prosecutor or code enforcement officer; confidentiality; definitions

A. Nothing in this chapter requires disclosure from a personnel file by a law enforcement agency or employing state or local governmental entity of the home address or home telephone number of a peace officer as defined in § 13-105, a justice, a judge, a commissioner, a public defender, a prosecutor or a code enforcement officer.

B. The agency or governmental entity may release the information in subsection A of this section only if either:

1. The person consents in writing to the release.

2. The custodian of records of the agency or governmental entity determines that release of the information does not create a reasonable risk of physical injury to the person or the person's immediate family or damage to the property of the person or the person's immediate family.

C. A law enforcement agency may release a photograph of a peace officer if either:

1. The peace officer has been arrested or has been formally charged by complaint, information or indictment for a misdemeanor or a felony offense.

2. The photograph is requested by a representative of a newspaper for a specific newsworthy event unless:

(a) The peace officer is serving in an undercover capacity or is scheduled to be serving in an undercover capacity within sixty days.

(b) The release of the photograph is not in the best interest of this state after taking into consideration the privacy, confidentiality and safety of the peace officer.

(c) An order pursuant to § 28-454 is in effect.

D. This section does not prohibit the use of a peace officer's photograph that is either:

1. Used by a law enforcement agency to assist a person who has a complaint against an officer to identify the officer.

2. Obtained from a source other than the law enforcement agency.

E. This section does not apply to a certified peace officer or code enforcement officer who is no longer employed as a peace officer or code enforcement officer by a state or local government entity.

F. For the purposes of this section:

1. "Code enforcement officer" means a person who is employed by a state or local government and whose duties include performing field inspections of buildings, structures or property to ensure compliance with and enforce national, state and local laws, ordinances and codes.

2. "Commissioner" means a commissioner of the superior court.

3. "Judge" means a judge of the United States district court, the United States court of appeals, the United States magistrate court, the United States bankruptcy court, the Arizona court of appeals, the superior court or a municipal court.

4. "Justice" means a justice of the United States or Arizona supreme court or a justice of the peace.

5. "Prosecutor" means a county attorney, a municipal prosecutor, the attorney general or a United States attorney and includes an assistant or deputy United States attorney, county attorney, municipal prosecutor or attorney general.

6. "Public defender" means a federal public defender, county public defender, county legal defender or county contract indigent defense counsel and includes an assistant or deputy federal public defender, county public defender or county legal defender.

§ 39-124. Releasing information identifying a peace officer, justice, judge, commissioner, public defender, prosecutor or code enforcement officer; violations; classification; definitions

A. Any person who is employed by a state or local government entity and who, in violation of § 39-123, knowingly releases the home address or home telephone number of a peace officer as defined in § 13-105, a justice, a judge, a commissioner, a public defender, a prosecutor or a code enforcement officer with the intent to hinder an investigation, cause physical injury to a peace officer, justice, judge, commissioner, public defender, prosecutor or code enforcement officer or the peace officer's, justice's, judge's, commissioner's, public defender's, prosecutor's or code enforcement officer's immediate family or cause damage to the property of a peace officer, justice, judge, commissioner, public defender, prosecutor or code enforcement officer or the peace officer's, justice's, judge's, commissioner's, public defender's, prosecutor's or code enforcement officer's immediate family is guilty of a class 6 felony.

B. Any person who is employed by a state or local government entity and who, in violation of § 39-123, knowingly releases a photograph of a peace officer with the intent to hinder an investigation, cause physical injury to a peace officer or the peace officer's immediate family or cause damage to the property of a peace officer or the peace officer's immediate family is guilty of a class 6 felony.

C. For the purposes of this section:

1. "Code enforcement officer" means a person who is employed by a state or local government and whose duties include performing field inspections of buildings, structures or property to ensure compliance with and enforce national, state and local laws, ordinances and codes.

2. "Commissioner" means a commissioner of the superior court.

3. "Judge" means a judge of the United States district court, the United States court of appeals, the United States magistrate court, the United States bankruptcy court, the Arizona court of appeals, the superior court or a municipal court.

4. "Justice" means a justice of the United States or Arizona supreme court or a justice of the peace.

5. "Prosecutor" means a county attorney, a municipal prosecutor, the attorney general or a United States attorney and includes an assistant or deputy United States attorney, county attorney, municipal prosecutor or attorney general.

6. "Public defender" means a federal public defender, county public defender, county legal defender or county contract indigent defense counsel and includes an assistant or deputy federal public defender, county public defender or county legal defender.

§ 39-125. Information relating to location of archaeological discoveries and places or objects included or eligible for inclusion on the Arizona register of historic places; confidentiality

Nothing in this chapter requires the disclosure of public records or other matters in the office of any officer that relate to the location of archaeological discoveries as described in § 41-841 or 41-844 or places or objects that are included on or may qualify for inclusion on the Arizona register of historic places as described in § 41-511.04, subsection A, paragraph 9. An officer may decline to release this information if the officer determines that the release of the information creates a reasonable risk of vandalism, theft or other damage to the archaeological discoveries or the places or objects that are included on or may qualify for inclusion on the register. In making a decision to disclose public records pursuant to this section, an officer may consult with the director of the Arizona state museum or the state historic preservation officer.

§ 39-126. Federal risk assessments of infrastructure; confidentiality

Nothing in this chapter requires the disclosure of a risk assessment that is performed by or on behalf of a federal agency to evaluate critical energy, water or telecommunications infrastructure to determine its vulnerability to sabotage or attack.

§ 39-127. Free copies of police reports for crime victims; definitions

A. A victim of a criminal offense that is a part i crime under the statewide uniform crime reporting program or an immediate family member of the victim if the victim is killed or incapacitated has the right to receive one copy of the police report from the investigating law enforcement agency at no charge.

B. For the purposes of this section, "criminal offense", "immediate family" and "victim" have the same meanings prescribed in § 13-4401.

Article 3. Lost Records

§ 39-141. Proof of certain lost or destroyed documents or instruments

Any deed, bond, bill of sale, mortgage, deed of trust, power of attorney or conveyance which is required or permitted by law to be acknowledged or recorded which has been so acknowledged or recorded, or any judgment, order or decree of a court of record in this state or the record or minute containing such judgment, which is lost or destroyed, may be supplied by parol proof of its contents.

§ 39-142. Action for restoration and substitution of lost or destroyed documents

Upon loss or destruction of an instrument as indicated in § 39-141, a person interested therein may bring an action in the superior court of the county where the loss or destruction occurred for restoration and substitution of such instrument against the grantor in a deed, or the parties interested in the instrument, or the parties who were interested adversely to plaintiff at the time of the rendition of judgment, or who are then adversely interested, or the heirs and legal representatives of such parties.

§ 39-143. Judgment of restoration; recording of judgment; judgment as substitute for original instrument

A. If upon the trial of the action provided for in § 39-142, the court finds that such instrument existed, and has been lost or destroyed and determines the contents thereof, it shall enter a judgment containing the finding and a description of the lost instrument and contents thereof.

B. A certified copy of the judgment may be recorded, and shall be substituted for and have the same force and effect as the original instrument.

§ 39-144. Recording of certified copies of lost or destroyed records or records of a former county

Certified copies from a record of a county, the record of which has been lost or destroyed, and certified copies from records of the county from which a new county was created, may be recorded in such county when the loss of the original has been first established.

§ 39-145. Re-recording of original papers when record destroyed

When the original papers have been preserved but the record thereof has been lost or destroyed, they may again be recorded within four years from the loss or destruction of such record. The last registration shall have force and effect from the date of the original registration.

Article 4. False Instruments and Records

§ 39-161. Presentment of false instrument for filing; classification

A person who acknowledges, certifies, notarizes, procures or offers to be filed, registered or recorded in a public office in this state an instrument he knows to be false or forged, which, if genuine, could be filed, registered or recorded under any law of this state or the United States, or in compliance with established procedure is guilty of a class 6 felony. As used in this section "instrument" includes a written instrument as defined in § 13-2001.

Appendix G
Model Memorandum of Understanding

The following Memorandum of Understanding (MOU) is included as a model form, and is not intended to be a complete or final document. Each Arizona Recorder that offers electronic recording of documents will need to revise and/or modify this model MOU to describe specific login parameters, transmission protocols, and other technical and legal requirements.

Insert County Seal

[Insert County name] COUNTY RECORDER'S OFFICE
[Insert County Recorder's Name], COUNTY RECORDER
[Enter address of County Recorder]

ELECTRONIC/DIGITAL RECORDING
MEMORANDUM OF UNDERSTANDING

THIS MEMORANDUM OF UNDERSTANDING, dated _____ is between _____**County** (Hereinafter "County" and _____ (hereinafter "Company" or "Third-Party Submitter").

_____ **County** desires to offer recording of real property documents by electronically receiving and transmitting documents electronically in substitution for conventional paper based documents and to assure that transactions are not legally invalid or unenforceable as a result of the use of available electronic technologies for the mutual benefit of the parties of the transactions.

For purposes of this Memorandum of Understanding, Electronic Recording is defined based on the level of automation and structure of the transaction. The three levels of automation are as follows:

> Level 1 Submitting organizations transmit scanned image original of ink signed documents to the county. The County completes the recording process in the same way as paper using the imaged copy as the source document. An electronic recording endorsement is returned to the organization in the form of a label or printing process in order for the submitting organization to append that information to the original paper document.
>
> Level 2 Submitting organizations transmit scanned images of ink signed documents along with electronic indexing information to the county. The County performs an

There will be no added fees or costs of any kind charged by the County for Electronic Recording.

County Requirements

The Electronic Recording Program of County is defined by the requirements attached to this Memorandum of Understanding.

Attachment A defines the technical specifications including format, levels of recording supported, transmission protocols, and security requirements of the electronic records required by County. Company agrees to provide the transmission to the County following the specifications outlined. Company understands that the specifications may change from time to time. In the event changes to the specification are required, the County will provide a written notice to the Company within a reasonable timeframe.

Attachment B contains the document and indexing specifications for the Electronic Recording program. For each document, the County specific document code is provided along with the required indexing information. Any County specific editing rules will also be described in this attachment. All indexing specifications must follow the Property Records Industry Association (PRIA) standards as set out on their website: http://pria.us.

Attachment C contains the processing schedules and hours of operation for the Electronic Recording Program. Neither party shall be liable for any failure to perform processing of the transactions and documents where such failure results from any act of Nature or other cause beyond the party's reasonable control (including, without limitation, any mechanical, electronic or communications failure) which prevents the parties from transmitting or receiving the electronic recording transactions. If the County system causes delays or power failures interfere with the normal course of business, the County will notify the affected Company with a choice of using a courier service or waiting until the problem has been remedied.

Attachment D provides the payment options supported for the Electronic Recording program.

Company/Third Party Submitter Responsibilities

Company acknowledges that Electronic Recording permits them to prepare, sign and/or transmit in electronic formats documents and business records and the document or records shall be considered as the "original" record of the transaction in substitution for, and with the same intended effect as, paper documents and, in the case that such documents bear a digital or electronic signature, paper documents bearing handwritten signatures.

By use of electronic or digital certificates to sign documents, Company intends to be bound to those documents for all purposes as fully as if paper versions of the documents had been manually signed.

By use of electronic or digital certificates to sign documents, Company intends to be bound by those electronic signatures affixed to any documents and such electronic signature shall have the same legal effect as if that signature was manually affixed to a paper version of the document.

By use of digital certificates to seal electronic files containing images of original paper documents or documents bearing manual signatures, Company shall recognize such sealed images for all purposes as fully as the original paper documents and shall be responsible for any failure by Users to comply with quality control procedures for assuring the accuracy and completeness of the electronic files.

The Company and/or its employees attest to the accuracy and completeness of the electronic records and acknowledge responsibility for the content of the documents submitted through the Electronic Recording Program. Should a dispute or legal action arise concerning an electronic transaction, the County will be held harmless and not liable for any damages.

Company is responsible for the costs of the system or services provided by a third party that enables Company to meet the Electronic Recording Program requirements.

General Understanding

The County will not incur any liability for the information electronically transmitted by the Company, included but not limited to any breach of security, fraud or deceit.

Neither the County nor Company shall be liable to the other for any special, incidental, exemplary or consequential damages arising from or as a result of any delay, omission or error in the Electronic Recording transmission or receipt.

The County and Company will attempt in good faith to resolve any controversy or claim arising out of or relating to Electronic Recording through either negotiation or mediation prior to initiating litigation.

Either party may terminate this Memorandum of Understanding for any reason by providing 30 days written notice of termination.

The County and Company acknowledge that the electronic recording process is an emerging technology and that State and National standards will continue to evolve. To further the technology and the electronic recording process, the County and Company will meet as needed to discuss changes and additions to this Memorandum of Understanding.

Agreed and Accepted:

By_____ (Company)

Signature_____

Print Name_____

Date_____

By _____ (Third Party Submitter)

Signature_____

Print Name _____

Date _____

By _____(County)

Signature_____

Print Name_____

Date_____

Customer Account #_____ (To be completed by County)

Attachment A
Technical Specifications

Format of the transmitted File

Property Records Industry Association (PRIA) http://pria.us/ Mortgage Industry Standards Maintenance Organization (MISMO) file format standard will be used http://www.mismo.org/default.htm. Any multi page storage format as specified by the County.

Communications Protocol and Options

Transmission Control Protocol/Internet Protocol (TCP/IP)

Security Framework

Encryption will be a minimum 128 bit file and image encryption. Secure Socket Layer (SSL) and user login/password will be employed. User passwords are controlled by the Company and should be monitored/or changed periodically to ensure security. Computers on which documents originate must have all critical operating system patches applied , must have a firewall (hardware or software) installed, and must have up to date virus scan software.

Returned File Format

Property Records Industry Association (PRIA)/Mortgage Industry Standards Maintenance Organization (MISMO) file format standard will be used. Any multi page storage format as specified by the County.

http://pria.us and http://www.mismo.org/default.htm

Levels of Electronic Recording Supported

Levels 1, 2, and 3 or as specified by the County.

Electronic Signatures and Use of Digital Certificates

The use of Electronic Signatures and Digital Certificates will need to adhere to the guidelines set out in E-Sign (please refer to federal statutes regarding this law) and Secretary of State administrative rules (http://www.azsos.gov/pa).

Imaging Standards

Documents will be scanned at a minimum of 300 dpi.
Documents will be scanned in portrait mode.
Document images will be captured in any multi page storage format as specified by the County.
Scanned documents will be legible so as to be able to reproduce onto microfilm or microfiche as required by law in A.R.S. § 11-480 – including signatures and notary seals.

Document font size must be 10 point or larger, margins will consist of a minimum of a 2" top margin and ½" side and bottom margins. NO DOCUMENTS WILL BE ACCEPTED THAT FAIL TO MEET THIS STANDARD (A.R.S. § 11-480).

Documents must be scanned to original size.

Attachment B
Documents and Indexing Specifications

Eligible Document Types

All document types and sizes must meet the requirements as set forth in A.R.S. § 11-480.

County Specific Document Type Coding

Please refer to PRIA website for the Logical Data Dictionary, which lists all the acceptable "Document Types". http://pria.us/ It is the County's intention to not reject documents based on "incorrect or non-County specific document types. Rather the County will correct the document type as part of the acceptance process.

Indexing Fields for each Document Code

All documents submitted will require the minimum index fields:

Grantor(s) or equivalent
Grantee(s) or equivalent
Document Type
Recording Fee
Related (original document number, in the case of releases, assignment, amendments, etc.).
Legal Description Fields as specified by County
Standard PRIA tags defined for these fields must be used. http://pria.us/

Affidavits of Value (AOV) per A.R.S. §§ 11-1133 and 11-1137(B).

AOV's will be scanned immediately following the Deed they are associated with. All Deeds will be accompanied by an AOV or an exemption code. Forms or exemption codes can be retrieved from this website. http://www.azdor.gov/Forms/property.asp
Standard MISMO tags defined for these fields must be used. http://www.mismo.org/default.htm

Document Imaging Quality Control Standards

Scanned documents will be legible so as to be able to reproduce onto microfilm or microfiche as required by law in A.R.S. § 11-480 – including signatures and notary seals. All documents must meet the recording requirements as set forth in A.R.S. § 11-480.

The xhtml document must display in W3C (World Wide Web Consortium) Standards.

Notary Requirements per Document

It is the responsibility of the Company to confirm that notary signatures and seals are present on all documents that require them.

Inked notary seals are strongly recommended, in place of embossed notary seals which require "darkening" by the Company prior to submittal.

All electronic notaries must adhere to the Secretary of State Standards for electronic notaries. http://www.azsos.gov/pa

Eligible Document Batches

Document batches will be submitted by a standard naming convention as specified by the County.

The maximum size of electronic document batches will be determined by the County.

Attachment C
Service Offering

Hours of Operation

Documents may only be submitted during the normal business hours of the County which is typically between 8 a.m. and 5 p.m., Mountain Standard Time. Documents will not be processed on federal or county holidays, weekends, snow days, declared emergencies, etc. or in the event of network or equipment failure. County will attempt to notify Company of any disruption in service.

Processing Schedules

Document batches must be received by 5:00 p.m. Mountain Standard Time to be recorded or rejected.

Return Options

Submitted documents that are accepted for recording will be made available to the Company in electronic format after recording.

Submitted documents that are rejected will be made available to the Company in electronic format after rejection, along with a description of the reason(s) for rejection.

Service Help Contact Information

County:

County eRecording Vendor:

Company:

Company eRecording Vendor:

Attachment D
Payment Options

Payment Options

Will be specified by County

Appendix H
Frequently Asked Questions

1. What are the minimum hardware requirements to implement eRecording?
2. What other requirements would there be?
3. What document types can be electronically recorded?
4. At which models may documents be received?
5. What is a SMART Doc™?
6. Why are standards important?
7. What are the three proven methods of delivery in eRecording?
8. How does the size of a county affect its ability to participate in eRecording?
9. What is the relationship between URPERA, UETA and E-SIGN?
10. What are the implications if Electronic Recording Commissions or state agencies overseeing the commission or committee adopt standards that are not aligned with the standards adopted by other states?
11. What types of output are generated by an Electronic Recording Commission?
12. Will the private industry solely drive the standards based on early adopters and the information they have already accumulated or will it be a collaborative effort by the early
    adopters from across the nation or state in both the private and public sectors?
13. What are significant national standards that guide eRecording today?
14. What is MISMO's relevance in eRecording?
15. What is PRIA's relevance in eRecording?
16. How much security is needed in eRecording?
17. What are the differences and benefits of digital signatures and digital certificates in eRecording?
18. Are digital signatures and electronic signatures the same?
19. What is the difference between a digital signature and a digitized signature?
20. What kinds of electronic signatures should be used? For which signatures?
21. How are electronic and paper documents meshed together?
22. Do current indexing standards also apply to electronic documents?
23. How can costs be reduced and controlled?
24. Are there more fraud concerns with electronic recording?
25. Can I use a sound as my signature?
26. How are recording fees paid?
27. Can a Recorder accept a document transmitted by facsimile for recording?
28. Will all Arizona counties accept electronic recording?

1. What are the minimum hardware requirements to implement eRecording?

   At a minimum, a county would need to have a server with enough disk space to enable a web services program. This program would typically be developed and provided by a vendor or portal solution at little or no cost to the county.

2. What other requirements would there be?

   The county would also need to have access to the Internet and have a web browser such as Internet Explorer, which is usually already included in the computer's packaged software when the unit was purchased.

3. What document types may be electronically recorded?

   All document types lend themselves to electronic recording. Plats or maps filed electronically may require special handling.

4. At which models can documents be received?

   Documents that can automatically be created by a template and have embedded index data submitted with the recording payload, and can be electronically signed and/or notarized, can be received by a Recorders if the Recorders system is capable of accepting model 3. Examples of these "Smart Docs" would be Satisfactions and possibly Assignments.

   Documents that require the original executed instrument to be recorded lend themselves to model 2 recording since an actual copy of the document with wet signatures must accompany the index data. Examples of this would be Deeds and Mortgages.

5. What is a SMART Doc™?

   A SMART Doc™ is found only on model 3 transactions. It gets its name from the fact that a human does not need to view or handle it for it to be recorded. SMART Docs™ contain all of the necessary information to create index entries and to electronically create a document that can be recorded. This indexing is accomplished by virtue of the submitter organizing and labeling the data payload in a standard format to which the recorder also subscribes.

6. Why are standards important?

   Standards are important because they allow various parties to communicate and understand each other in a predefined manner. Without standards there would be constant interpreting and deciphering of information. In the eRecording world standards allow each party to organize and submit data to the other in a universal manner, without having to employ the use of custom integration points, and in order to facilitate interstate communication.

7. What are the three proven methods of delivery in eRecording?

   The three methods are point-to point-integration, third party vendor, and a portal. In the beginning when eRecording was a new concept, the third party vendor method was popular due to the lack of document preparation software available at the submitter's site.

   As eRecording's popularity caught on submitters sometimes found it beneficial to eliminate the costs of a third party vendor and develop a point-to-point integration directly

with the county. This was typically true with larger counties where greater recording volumes are common.

Inherent with many submitters trying to send to many counties and not wanting to develop unique integration and data schemes for each, the concept of a portal was born. The portal was designed to be a central clearinghouse for submitters and counties. As proven, a submitter can deliver various documents intended for several different counties nationwide to the portal. The portal has the ability to verify that specific county index standards have been met and then deliver each document to the specific county for which it is intended.

8. How does the size of a county affect its ability to participate in eRecording?

Because there are many methods in which to participate, a county's size has little bearing on its ability to implement eRecording. A small county that has Internet access could use a web services program to receive and return documents. A medium or large county that has more volume could use a vendor solution or agree to a point-to-point integration directly with the submitter. A portal could be used with any size county since the portal doesn't care or factor in the size of a county to perform its functionality, or to deliver and return recorded documents from that county.

9. What is the relationship between URPERA, UETA and E-SIGN?

E-SIGN and UETA are federal and uniform state laws, respectively, enacted to enable electronic commerce. While E-SIGN covers some additional issues, they are complementary acts. They are similar in their application to electronic documents and electronic signatures based on voluntary agreement between parties. Both are self-implementing. Between them they remove barriers on both interstate and intrastate levels. E-SIGN explicitly preempts certain state laws that do not conform to E-SIGN even where a state enacts UETA.

URPERA is a follow up act to UETA with the purpose of clarifying ancillary recording issues. It also establishes a method for adopting standards on a statewide basis that has the potential for implementing uniform standards nationally.

10. What are the implications if Electronic Recording Commissions or state agencies overseeing the commission or committee adopt standards that are not aligned with the standards adopted by other states?

Since mortgage lending and title insurance have become national businesses that are utilized by citizens, this is a significant question. Adopting multiple standards that are not aligned will result in higher costs for both document submitters and county recorders. Computer systems for mortgage lenders, attorneys, settlement agents, title insurance companies and county recorders will have to be designed to accommodate multiple sets of standards. Each different set will need to be mapped to the MISMO standards used by the industry. Even then, with incompatible specifications mapping may be inadequate.

Current national standards are driven by the private sector needs of interoperability among trading partners. Standards developed by PRIA reuse industry (MISMO) architecture, structure and data points. Likewise, MISMO reuses PRIA standards for those pieces unique to recording.

11. What types of output are generated by an Electronic Recording Commission?

    Document deliverables can be in two forms. One is to generate the standards, even if adopting from sources such as PRIA, in the format of XML Document Type Definitions (DTDs) or schema, data dictionaries, implementation guides, etc. The other is to issue compiled references to adopted specifications, citing the source and location of the specifications adopted.

12. Will the private industry solely drive the standards based on early adopters and the information they have already accumulated or will it be a collaborative effort by the early adopters from across the nation or state in both the private and public sectors?

    The latter. Standards development has already been a collaborative effort, both by trading partners in the private sector and county recorders. However, the collaboration includes more than early adopters. A number of large entities have participated in the standards process even though they have not yet implemented electronic transaction solutions.

13. What are significant national standards that guide eRecording today?

    PRIA eRecording; PRIA Notary; MISMO Closing, Servicing, Origination, Request and Response envelopes, eMortgage SMART Doc™, eMortgage eRegistry, eMortgage ePackage; PDF, TIFF; XML.

14. What is MISMO's relevance in eRecording?

    MISMO is the primary standards setting body for the financial services organizations where the lending process begins and whose work efforts result in recordable documents. Their standards will be used by those organizations to create documents and share data. Since this group includes those who create the vast majority of documents to be recorded, their standards will be a major factor in documents processed by county recorders.

15. What is PRIA's relevance in eRecording?

    PRIA is a public/private cooperative entity with both recorders and submitters among its members. Its mission is to create and maintain standards. Four technical standards have been developed specific to electronic recording by PRIA. Two are envelopes for submitting and returning recordings. A third is the specification for the document information. The final specification is for notarial information included in notarial certificates and incorporates notary signatures and commission information.

    The PRIA technical specifications were developed in close coordination with the private sector (MISMO) to ensure the interoperability of the technical standards. In fact, PRIA reuses a number of the data elements developed by MISMO and as well as the MISMO architecture. In turn, MISMO has adopted the PRIA data elements specific to recording for incorporation into its data dictionary and technical specifications.

    Ultimately, widespread adoption of a standard will facilitate electronic commerce in the real estate finance industry. Neither the private nor the public sector can afford applications that accommodate different interfaces with each different trading partner or customer. PRIA offers a universal interface for recorders that submitters can rely on.

16. How much security is needed in eRecording?

Security is a matter of quality rather than quantity. The quality must be sufficient to protect the assets to the degree that it covers the risk inherent in the process. Once completed the documents will be public record, so protection against prying eyes is not a high priority. On the other hand, documents must be secure from interception that results in their being delayed or not delivered, from substitution by different documents, or from alteration. And because recordings include payment of fees and taxes, the payment system must be secured.

Recorders need to prevent viruses, worms, Trojan horses and other malicious software from infecting their networks and systems. They also need to ensure unauthorized parties do not gain access to the parts of their networks that are not authorized to be accessed by the public.

It is not the Recorders' responsibility to ensure the accuracy or legality of the documents themselves, except insofar as they qualify to be recorded. Security for that lies outside the scope of recording.

17. What are the differences and benefits of digital signatures and digital certificates in eRecording?

Digital signatures enable both the recorders and the submitters to determine whether a document or set of documents was altered so they can decide whether or not to continue the process or rely on the resulting recording. While digital signatures require signers to use a key they control to complete the signature, the resulting signatures do not identify the signers in the same manner that a signature on a paper document is identifiable.

Digital certificates can provide a model of certainty that the signers are who they claim to be, thus providing a degree of trust. From a security aspect this can be an important tool insofar as the recorders can use it to decide who to accept documents from. Conversely, submitters or other parties can determine that particular recordings are authentic when documents are returned from the recorder's office with endorsement of recording information.

18. Are digital signatures and electronic signatures the same?

Yes and no. A digital signature is a kind of electronic signature. Not all electronic signatures are digital signatures in the same way not all pens are fountain pens.

19. What is the difference between a digital signature and a digitized signature?

As described in the Glossary found in Appendix A:

Digital signature: A complex string of electronic data that contains encoded information about a document and the person who signed it. Because they use powerful asymmetric encryption technology, digital signatures are the most secure type of electronic signature.

Digitized signature: A scanned image of a person's handwritten signature, which is captured using special digitizing hardware and stored as a computer file.

20. What kinds of electronic signatures should be used? For which signatures?

    This is a matter of agreement between parties, except as to government entities that may have the authority to establish performance standards for signatures under certain circumstances. Even so, government entities need to exercise caution that one technology is not given a higher legal standing than others. E-SIGN claims preemption in such cases.

21. How are electronic and paper documents meshed together?

    The concept of "meshing" electronic and paper documents together does not really exist. Once the electronic document is received into the Recorder's system, the process of calculating fees, assigning time, book & page, instrument numbers is the same as for paper documents. Depending on the model of the electronic document, the image may be transported automatically into the Recorder's system for public retrieval alongside the paper document that was scanned by Recorder's staff.

22. Do current indexing standards also apply to electronic documents?

    Recorders have the same responsibility for indexing documents received electronically as paper documents received in person, by U.S. mail, and by express methods.

23. How can costs be reduced and controlled?

    One option being studied is the establishment of a "portal" that would accept documents submitted electronically from ANY system and transmit those documents to the appropriate register's office, no matter what vendor they use for their back end system. This concept would eliminate the need for specific software between a submitter and each recorder with whom they file. Different versions of the "portal" concept are being used in other states, some more successfully than others.

24. Are there more fraud concerns with electronic recording?

    There is less chance of a document being altered at the recording counter or en route to Recorders offices than might exist during the prior activities which occurred in the attorney's or title offices. Moreover, intentional fraud is a moral issue and will not be controlled by recording statutes or methods.

25. Can I use a sound as my signature?

    URPERA authorizes the use of many types of electronic signatures. A county's memorandum of understanding will detail what technology is supported by that county.

26. How are recording fees paid?

    Fees are to be collected according to statute and in a manner consistent with the promotion of electronic recording, and in accordance with accepted industry standards. Each county recorder may collect electronic recording fees in a manner compatible with its internal software and county financial practices. (See Standard 7 for more information.)

27. Can a Recorder accept a document transmitted by facsimile for recording?

    No, a facsimile is an electronic document without an electronic signature, and does not

include the requisite transactional and organizational security standards to be accepted for recording.

28. Will all Arizona counties accept electronic recording?

No, A.R.S. § 11-487.03 provides that implementation of electronic recording is optional county by county.