ARIZONA *DEPARTMENT* *OF* *ADMINISTRATION*	**Statewide** POLICY	**State of Arizona**

POLICY 4070: ELECTRONIC AND DIGITAL SIGNATURE POLICY

DOCUMENT NUMBER:	**4070**
EFFECTIVE DATE:	**DECEMBER 2018**
REVISION NUMBER:	**1.1**

1. AUTHORITY

1.1 To effectuate the mission and purposes of the Arizona Department of Administration (ADOA), ADOA shall establish a coordinated plan and program for information technology (IT) implemented and maintained through policies, standards and procedures as authorized by Arizona Revised Statutes (A.R.S.) § 18-104.

Pursuant to A.R.S. § 18-106 (A), ADOA, in consultation with the State Treasurer, shall adopt policies and rules pursuant to Title 41, Chapter 6 establishing policies and procedures for the use of Electronic and Digital Signatures by all State Agencies, Boards and Commissions for Records[1] filed with and by all State Agencies, Boards and Commissions.

Under A.R.S. § 44-7042, "State agencies shall accept electronic records and electronic signatures" and shall comply with the policies adopted by ADOA pursuant to A.R.S. § 18-106.

2. PURPOSE

2.1 The purpose of this document is to establish, in accordance with A.R.S. § 18-106, a statewide policy concerning the use of electronic and digital signatures technology. It provides guidance to State Budget Units (BU) to evaluate new and existing electronic signature technology. The goal is for BUs to determine and assess the benefits and risks of using Electronic Signatures, determine whether their use is appropriate for their business needs, and ensure that they can be used within these technology guidelines. Except to the extent electronic or digital signature technology is utilized, this policy does not provide guidance on a BU's business process or business needs, as such are outside the scope of ADOA's authority.

[1] A.R.S. § 18-106 (F)(8) defines a "Record" as "information that is inscribed in a tangible medium or that is stored in an electronic or other medium and is retrievable in a physically perceivable form. Record includes electronic records and printed, typewritten and tangible records."

2.2 This policy does not provide guidance regarding notaries public and electronic notarization laws under Title 41, Chapter 2, as such are outside the scope of ADOA's authority

3. SCOPE AND APPLICABILITY

3.1 This policy applies to all State Budget Units (BUs).

3.2 Applicability of this policy to third parties is governed by contractual agreements entered into between the BU and the third party. For contracts in force as of the effective date, subject matter experts (SMEs) shall review the applicability of this policy to third parties before seeking amendments. Prior to entering into new contracts, SMEs shall ascertain the applicability of this policy to third parties and include compliance requirements in the terms and conditions.

3.3 With respect to all other Information Systems in service as of the Effective Date, implementation of this policy is recommended but is not mandatory. If such systems are already compliant as of the Effective Date, procedures to keep them compliant for the remainder of their lifetime should be implemented or continued.

3.4 This policy shall be referenced in Business Requirements Documents, Requests for Information, Requests for Proposal, Statements of Work and other documents that specify the business and technical specifications of Information Systems being developed, maintained, or procured.

3.5 State BUs and third parties supplying information systems to other BUs or developing information systems on behalf of a BU shall be required to comply with this Policy including documentation to demonstrate compliance with all State policies and documented security controls.

4. EXCEPTIONS

4.1 In the event that a BU takes exception to Sections 6.2 and 6.4 of this policy, then the BU shall assume all risks of non-compliance with this policy as written.

5. ROLES AND RESPONSIBILITIES

5.1 The Chief Executive Officer of the BU or his/her designee shall ensure the effective implementation of Information Technology Policies, Standards, and Procedures (PSPs) within the BU.

5.2 BU Supervisors shall ensure that employees and contractors are appropriately trained and educated on this Policy and shall monitor employee and contractor activities to ensure compliance.

5.3 Employees and contractors shall adhere to all state and BU policies, standards and procedures pertaining to the use of the State IT resources.

6. POLICY

6.1 BUs shall determine on a case-by-case basis whether a given process requiring a signed Record can utilize an Electronic Signature, or whether it requires the additional rigor and security of a Digital Signature. For most processes, an Electronic Signature can be used, and a Digital Signature is not necessary. For some processes, a Digital Signature is specifically required by law or necessary to protect high risk, high value processes.

6.2 If a BU uses an Electronic Signature for a given process, the BU shall implement a process that satisfies all of the following minimum requirements:

6.2.1 The process implemented shall satisfy all the applicable requirements of A.R.S. § 18-106, including that:

a. Each Electronic Signature shall be unique to the person using it.

b. Each Electronic Signature shall be capable of reliable verification.

c. The process implemented shall not allow an electronically signed Record to be altered without invalidating the signature, or the Record shall maintain, within the data set, evidence that the Record was deleted or altered after signature

6.2.2 An unaltered, fully executed, complete electronic copy of the Record shall be made available to all parties for their reference and archiving.

6.2.3 All electronically signed Records shall be retained in accordance with the record retention policies prescribed by the Arizona State Library, Archives and Public Records Division of the Arizona Secretary of State.

6.3 While not required by statute, in order to evidence compliance with A.R.S. § 18-106, BUs may implement one or more of the following practices and controls for a process that uses Electronic Signatures:

6.3.1 Consent of the Parties: Parties do not have to expressly agree for an Electronic Signature to be effective, and consent can be implied from the parties' actions in transacting electronically. BUs may add a consent provision in the electronically signed Record.

6.3.2 Audit Trail: A signature audit trail provides clear evidence of the signing process, such as the date, time, location, and/or identity of all signers.

6.3.3 Disinterested Third Party: The BU may have the signing process facilitated or conducted by a third party who does not have an interest in the BU's given process.

6.3.4 Email Account, if applicable: If a signer has an email account under his/her control that is known to the BU, then the BU may link the signing process to that email account.

6.3.5 Two-Factor Authentication, if necessary: If the BU determines that a process has moderate risk, then the BU can use this enhanced process, which adds a signer authentication challenge before a Record can be signed to verify the signer's identity. A signer authentication challenge can include a personal identification number (PIN), password, or knowledge-based authentication (KBA).

6.4 In the event that a BU determines that a given process requires the additional rigor and security of a Digital Signature, then in such event, the tool, software, service and process that performs the Digital Signature shall comply with Federal Information Processing Standards (FIPS) Publication 186-4 for the Digital Signature Standard (DSS).

7. DEFINITIONS AND ABBREVIATIONS

7.1 The Glossary of Terms, Acronyms and Mathematical Symbols of FIPS Publication 186-4 is incorporated herein by reference.

7.2 The Definitions cited in A.R.S. § 18-106 (F) are incorporated herein by reference. Definitions in this policy are intended to refine, and not replace, definitions in that statute.

7.3 If a term is defined differently between A.R.S. § 18-106 (F) and FIPS Publication 186-4, then the definition in A.R.S. § 18-106 (F) shall prevail.

~~**7.4** Refer to the PSP Glossary of Terms located on the ADOA-ASET website.~~

7.5 Electronic Signature is an electronic sound, symbol, or process attached to or logically associated with a Record and executed or adopted by a person with the intent to be bound by or to authenticate a Record. The term "electronic signature" is often confused with that of a "digital signature." However, a Digital Signature (defined below) is a specific type of electronic signature. The definition for "electronic signature" is not technology-specific; it does not require the use of any particular hardware or software application, but allows for any technology that can properly authenticate the signer and the signed Record.

7.6 Digital Signature is a type of electronic signature that relies on a public key infrastructure (PKI) to provide a unique identifier and link the signature to the Record, authenticating both the signer and the Record. Public key infrastructure technology is based on a "key pair" managed by a trusted third party called a "certification authority." A private key belonging to the sender is used to create the signature, and a mathematically-related public key made publicly available is used by the recipient to validate the authenticity of the signature. A mathematical operation combines the content of the message and the signer's private key to attach the resulting digital signature to the original message. This process 1) authenticates the signer, since only the signer should have access to both the private key and the message; and 2) verifies the integrity of the original message, since any subsequent changes to the message would invalidate the signature.

8. REFERENCES

ADOA-P1000, Information Technology Policy
A.R.S. § 18-104
A.R.S. § 18-106
FIPS Publication 186-4

9. ATTACHMENTS

None.

10. Revision History

Date	Change	Revision	Signature
06/01/2017	Draft created	0.1	Deirdre LaGuardia
06/23/2017	Peer Review	0.2	Justin Turner
06/30/2017	Revisions	0.3	Jeff Wolkove, Nicole Ong Colyer, Justin Turner & Deirdre LaGuardia
7/12/2017	Renumbered to 4070 to conform to Collaboration and Communication policy numbering sequence	0.4	Jeff Wolkove
8/10/2017	Revised to accommodate suggestions from reviewers	0.5	Jeff Wolkove, Nicole Ong-Colyer
9/12/2017	Revised to add guidance	0.6	Jeff Wolkove, Nicole Ong-Colyer
10/18/2017	Revised to accommodate suggestions from reviewers	0.7	Nicole Ong-Colyer
11/01/2017	Finalized	1.0	Morgan Reed

APPROVED BY THE STATE CHIEF INFORMATION OFFICER AND EFFECTIVE AS OF NOVEMBER 1, 2017.
Morgan Reed

Signature: Email: Morgan Reed (Oct 30, 2017) morgan.reed@azdoa.gov