

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

STATEWIDE POLICY P4060: ELECTRONIC AND DIGITAL FILE MANAGEMENT

DOCUMENT NUMBER:	STATEWIDE-P4060
EFFECTIVE DATE:	XXXXXXXX
REVISION:	0.1

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Administration (ADOA), the Agency 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 specified in ADOA Information Technology Policy ADOA – P1000 and consistent with Statewide Information Technology policies and standards. The authority of the ADOA to develop and enforce IT policies is derived from A.R.S. § 41-3504.

2. PURPOSE

The purpose is to establish a Budget Unit (BU) policy that facilitates the proper creation, management, preservation and disposal of public records in the form of electronic and digital files in accordance with A.R.S. § 41-151.12.

3. SCOPE

3.1 Applicability to individuals and BUs - This policy applies to all employees and contractors within a BU who generate public records in the form of electronic and digital files while executing their business functions, activities or services for or on behalf of the BU.

3.1.1 All individuals subject to this policy should be aware that electronic and digital files are subject to public record requests under the Arizona Inspection of Public Records Law (A.R.S. § 39-121), litigation holds and legal discovery when a lawsuit is pending. Should electronic and digital files that are the subject of a public request, litigation holds or legal discovery be deleted as a result of improper management, the BU risks facing severe court sanctions and/or a criminal charge.

- 3.1.2** All individuals subject to this policy who willfully contravene the electronic and digital file management provisions in this policy shall face disciplinary action.
- 3.1.3** This policy shall not be construed to supersede any federal or State laws or statutes related to electronic and digital files with respect to content, retention, individuals, or groups.
- 3.2 Third Parties** - Applicability of this policy to third parties is governed by contractual agreements entered into between the BU and the third party. For existing contracts, subject matter experts (SMEs) should ascertain 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 before including compliance requirements in the terms and conditions.
- 3.3 Applicability to electronic and digital files as public records** - An electronic and digital file is a public record if it meets the criteria defined in A.R.S. § 41-151.18.
 - 3.3.1** Electronic and digital files are created as a result of on-boarding an individual into the BU, a delegate, a group with an owner, or through automated procedures within applications.
 - 3.3.2** Electronic and digital files from individuals/groups/system shall be terminated as a result of off-boarding, deletion of a group, suspension/termination of automated procedures within applications. Such electronic and digital files shall be redirected to appropriate owner(s) for public records management purposes following off-boarding procedures.

4. EXCEPTIONS

All requests for exceptions to this policy should be directed to the Records Management Division of Arizona State Library, Archives and Public Records (ASLAPR) after consultation with the legal counsel.

5. ROLES AND RESPONSIBILITIES

5.1 BU Director or Designee is Responsible for:

- a.** Approval of this policy and for the designation of a senior manager as the electronic and digital file records manager. Executive management shall mandate the electronic and digital files records manager to implement this policy;
- b.** Ensuring that the management of public records including electronic and digital files is a key responsibility of all managers;
- c.** Implementation of this policy in their respective units. They shall ensure that the management of public records including electronic and digital files are a key responsibility of all individuals subject to this policy in their units; and

- d. Leading by example and shall ensure that public records, including electronic and digital files generated by them are managed in accordance with A.R.S. § 41-151.12.

5.2 Public Information Officer or Designee is Responsible for:

- a. All communications, both internal and external, related to the electronic and digital file public record keeping and public records management practices of the BU.

5.3 Legal Counsel or Designee is Responsible for:

- a. Updating the Records Manager regarding developments in the legal and statutory environment that may impact on the record keeping and public records management practices of the BU.

5.4 Records Manager or Designee is Responsible for:

- a. The implementation of this policy;
- b. Communicating electronic and digital file classification rules;
- c. Communicating clear and concise details relating to electronic and digital file management expectations for each electronic and digital file classification type;
- d. Ensuring awareness by all individuals subject to this policy;
- e. Ensuring that electronic and digital files are managed as public records according to the public records management principles prescribed by A.R.S. § 41-151.12 and in terms of this policy. In this regard the records manager shall be consulted to determine which types of electronic and digital files would be considered official public records that should be managed properly;
- f. Ensuring that all electronic and digital file public records created and received by the BU are classified according to the approved classification policy (P8110 – Data Classification Policy Framework) and that a written disposal authority is obtained for them from ASLAPR;
- g. Determining retention periods in consultation with the risk manager, the legal services manager and the users and taking into account the functional, legal and historical need of the body to maintain public records of transactions;
- h. Mandating such training and other interventions as are necessary to ensure that the BU's electronic and digital file public record keeping and public records management practices comply with the public records management principles contained in A.R.S. § 41-151.12;

- i. Issuing circulars and instructions regarding electronic and digital file public record keeping and public records management practices of the BU;
- j. Informing the Chief Information Officer if a request for information necessitates a disposal hold to be placed on public records that are due for disposal;
- k. In conjunction with the Chief Information Officer, transferring electronic and digital files that are deemed to be permanent to Records Management Division of ASLAPR; and
- l. Monitoring the implementation of this policy.

5.5 Chief Information Officer or Designee is Responsible for:

- a. Fulfilling requests for information in electronic format pursuant to Arizona Inspection of Public Records Law (A.R.S. § 39-121);
- b. The day-to-day maintenance of electronic systems that store public records including the (hardware/software) that serves as the conduit for receiving and transmitting electronic and digital files;
- c. Working in conjunction with the Agency Records Manager to ensure that public records are managed, protected and appropriately preserved for as long as they are required for business, legal and long-term preservation purposes;
- d. Ensuring that Agencies report the destruction of public records without legal, administrative, historical, or other value to ASLAPR on an annual basis (A.R.S. § 41-151.15);
- e. Consulting with the Records Manager prior to deleting any electronic or digital files that are deemed to be records (A.R.S. § 41-151.15.B);
- f. Ensuring that the integrity of any public record housed in the electronic and digital file format is protected until they have reached their approved retention. Integrity of these public records will be accomplished through such procedures as test restores, media testing and data migration and capturing the required audit trails;
- g. Ensuring that appropriate systems technical manuals and systems procedures manuals are designed for each electronic system that manages and stores public records;
- h. Ensuring that all electronic systems capture appropriate systems generated metadata and audit trail data for all electronic and digital files to ensure that authentic and reliable public records are created;

- i. Ensuring that electronic and digital files in all electronic systems remains accessible by migrating them to new hardware and software platforms when there is a danger of technology obsolescence including media and format obsolescence;
- j. Ensuring that all electronic and digital files data, metadata, audit trail data, operating systems and application software are backed up on a daily, weekly and monthly basis to enable the recovery of authentic, reliable and accessible public records should a disaster occur;
- k. Ensuring electronic and digital file management commences during individual on-boarding and transitions during off-boarding as per procedures;
- l. Ensuring that the archive files for the electronic and digital file system are recognized as being part of the overall public records management system in that the subject classification scheme shall be evident if files need to be retrieved from the archives;
- m. Ensuring that backups are stored in a secure environment with recovery capabilities including from disasters; and
- n. Ensuring that systems that manage and store public records are virus free.

5.6 Security Manager or Designee is Responsible for:

- a. The physical and logical security of all public records; and
- b. Details regarding the specific responsibilities of the security division contained in the Statewide Information Security Policy Framework, P8120.

5.7 All Individuals Subject to this Policy:

- a. Are responsible for ensuring that electronic and digital files, that are evidence of business transactions, are captured as public records; and
- b. Are responsible for ensuring that electronic and digital files are subject to classification in accordance with the approved standards.

6. STATEWIDE POLICY

- 6.1** All electronic and digital files created and received by the BU shall be managed in accordance with the public records management definition contained in A.R.S. § 41-151.14.D, guidelines that are established by the Director, Arizona State Library, Archives and Public Records pursuant to §41-151.14, and other jurisdictions (if applicable).

- 6.2** The following broad principles apply to the electronic and digital file public record keeping and public records management practices of the BU:
- a. Follow sound procedures for the creation, maintenance, retention and disposal of electronic and digital file public records.
 - b. The public records management procedures of the BU shall comply with legal requirements, including those for the provision of evidence.
 - c. The BU shall follow sound procedures for the security, privacy and confidentiality of its electronic and digital file public records.
- 6.3** The BU shall implement performance measures for all electronic and digital file public records management functions and review compliance with these measures as established by the Director, ASLAPR pursuant to A.R.S. § 41-151.15.
- 6.4** All individuals subject to this policy shall observe public records laws and associated public records retention requirements for electronic and digital files.
- 6.4.1 Retaining electronic and digital files** - Electronic and digital file retention is governed by A.R.S. § 41-151.12.
- 6.4.1.1 Electronic and digital files shall under no circumstances be isolated from the BU's public records management systems.
 - 6.4.1.2 Demonstrable inability to tamper with electronic and digital files and related metadata shall be implemented.
 - 6.4.1.3 Electronic and digital files under litigation hold shall be placed on legal hold following legal requirements.
 - 6.4.1.4 Each electronic and digital file shall be retained based on clearly defined policy and retention schedule(s).
- 6.4.2 Electronic and Digital File Disposal** - Electronic and digital files considered to be public records shall not be deleted or otherwise disposed of without a written disposal authority issued by ASLAPR.
- 6.4.2.1 Disposal of electronic and digital files are governed pursuant to A.R.S. § 41-151.12.
 - 6.4.2.2 Electronic and digital files that are not public records may be disposed, pursuant to A.R.S. § 41-151.12.

6.4.3 Electronic and Digital File Restoration - Deleted electronic and digital files can be restored within 14 days of deletion. After 14 days, deleted electronic and digital files will be permanently expunged from the system.

7. DEFINITIONS AND ABBREVIATIONS

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

8. REFERENCES

- 8.1** Statewide Policy Framework P1000 Information Technology
- 8.2** A.R.S. § 41-3504 Powers and duties of the department; violation; classification
- 8.3** A.R.S. § 39-121 Arizona Inspection of Public Records Law
- 8.4** A.R.S. § 41-151.18 Definition of Records
- 8.5** A.R.S. § 41-151.14 State and local public records management; violation; classification; definition
- 8.6** A.R.S. § 41-151.15 Preservation of public records
- 8.7** A.R.S. § 41-151.12 Records; records management; powers and duties of director; fees; records services fund
- 8.8** Statewide Policy Framework P8110 Data Classification Policy
- 8.9** Statewide Policy Framework P8120 Information Security Program Policy
- 8.10** Arizona Public Records Law published by Arizona Ombudsman

9. ATTACHMENTS

None.

10. REVISION HISTORY

Date	Change	Revision	Signature
10/24/2019	Draft	0.1	Simone Berg, ADOA-ASET Knowledge Manager