

ARIZONA CODE OF JUDICIAL ADMINISTRATION
Part 1: Judicial Branch Administration
Chapter 5: Automation
Section 1-507: Protection of Electronic Records in Paperless Court Operations

A. Definitions. In this section, the definitions set out in section 1-504 apply. In addition:

“Administrative record” means any record created or received by a court that does not pertain to a particular case or controversy filed with a court. Administrative records include any record maintained by any board, committee, commission, council, or regulatory body, including records of the regulation and discipline of attorneys.

“Case management system” (CMS) means the information system that captures, maintains and provides access to data related to court cases over time, enabling systematic control of records through their lifecycle. It is often connected to a document management system that stores case-related documents electronically.

“Case record” means any record pertaining to a particular case or controversy.

“Closed case” means any case file record that is no longer subject to modification.

“Cloud-hosted” refers to data storage or computer applications that reside on remote servers outside of court premises and accessible using the Internet.

“Courts” means courts or clerks of court.

“Electronic record” means any record that requires the aid of a computer to be read, including imaged documents and files, whether stored in an EDMS or a CMS.

“Electronic Archive” means an electronic document repository consisting of imaged or e-filed documents associated only with closed cases.

“Electronic document management system (EDMS)” means a collection of computer software application programs and hardware devices that provides a means of organizing and controlling the creation, management, and retrieval of documents through their life cycle.

“Offsite” means a temperature-controlled storage location physically located sufficient distance away from the main storage environment that an adverse event that affects the one does not affect the other.

“Online” means the storage of digital data on magnetic disks (such as hard drives) to make it directly and quickly accessible on the network using the application associated with the data.

~~“RAID” means Redundant Array of Independent Disks, a data storage system made of two or more ordinary hard disks and a special disk controller. Various RAID levels exist including RAID 1 which mirrors disks for fault tolerance and RAID 5 which stripes a set of disks for~~

~~increased performance with fault tolerance.~~

“Regulatory case record” means any record that pertains to the regulation of a particular professional or business registered, licensed or certified pursuant to rules adopted by the supreme court.

“Storage” means a permanent repository for holding digital data that retains its content until purposely erased, even when electrical power is removed.

B. and C. [No change]

D. Requirements Applicable to Case Records.

1. General Requirements.

- a. through d. [No change]

2. Document Management Requirements.

- a. Courts shall use an electronic document management system (EDMS) that complies with ACJA § 1-505, or be granted an exception by Commission on Technology to use a non-conforming system.
- b. ~~The~~ If not cloud-hosted, EDMS application data shall reside on at least two physically separate servers each using separate internal storage, structured query language (SQL) databases, and backup software. Log shipping Replication shall be employed not less than daily to maintain synchronization of the two EDMSs application data stores for disaster recovery purposes.
- c. At least six months of full-time production use of an EDMS is required before a court may request authorization to begin destroying the paper records corresponding to electronic records stored on the system, as required by ~~subsection~~ paragraph (F) of this section.

3. Storage Requirements.

- a. If not cloud hosted, ~~C~~courts shall maintain primary and secondary copies of records online at all times using at least two physically separate storage ~~arrays~~ devices configured to ~~as~~ensure the failure of any single component of the array will not impact the integrity of the data. New records shall be written simultaneously to all disk arrays. Data replication must be in as near-real-time as possible, not to exceed 30 minutes, within the available network constraints.
- b. For on-premises systems, ~~P~~primary and secondary storage shall be designed with redundant hardware and software to support fast recovery of data. attached only to servers having redundant power supplies, network interface cards, and controller cards

~~or to virtual servers having automatic failover hosts.~~ Use of personal computers containing extra hard drives or attached storage devices is prohibited.

- c. Courts shall use redundant network paths to connect workstations and imaging devices to EDMS application servers.
- d. For on-premises systems, ~~C~~courts shall employ uninterruptable power supplies and software that ensure a controlled shutdown of servers after batteries have been in use for at least five minutes.
- e. Courts shall store a tertiary copy of records on highly-secured, immutable backup media. The tertiary copy shall only be accessed through a gateway technology that prevents direct access to the storage media from the system(s) being backed up. Manufacturer's usage specifications and backup system media replacement guidelines shall be followed at all times, in accordance with ACJA § 1-504(G)(2).
- f. At a minimum, the tertiary backup shall be performed daily using automated backup software.
- ~~f.g.~~ Backups ~~media~~ shall be stored in a secure, environmentally controlled, offsite location and retained a minimum of 28 days ~~offsite before reuse~~. Full backups ~~shall~~ should be made not less than weekly and retained a minimum of 28 days offsite ~~before reuse~~.
- ~~g.h.~~ Backup and restoration procedures shall be documented and tested for effectiveness.
- ~~h.i.~~ Scanned records shall appear on the backup media as well as primary and secondary storage before corresponding paper is destroyed.

4. [No change]

5. Support and Maintenance Requirements.

- a. At least one Ccourt employee personnel or contractors must hold a current Hyland Certified OnBase Administrator Expert credential or equivalent certification, including for any approved, non-conforming EDMS.~~be certified in the following areas required to proficiently operate and maintain the records management system:~~
 - ~~(1) Microsoft Certified Systems Administrator~~
 - ~~(2) Microsoft Certified Database Administrator~~
 - ~~(3) OnBase Certified Advanced System Administrator or equivalent for any approved, non-conforming EDMS.~~
- b. through f. [No change]

E. Requirements Applicable to Administrative and Regulatory Case Records. Requirements

applicable to case records in paragraph (D) apply to administrative and regulatory case records with the following modifications.

1. If not cloud-hosted, ~~t~~The EDMS application may reside on one server, rather than two separate servers.
2. Copies of the records may be limited to one primary copy and one backup copy. The primary copy of all electronic records shall be maintained online at all times ~~using at least one RAID Level 5 disk or storage array.~~
- ~~3. The server on which the EDMS application and records reside shall, at a minimum, be attached to or contain magnetic storage in a RAID Level 1 configuration.~~
- ~~4.3.~~ Servers used for an electronic archive shall be ~~installed in a rack or other fixture~~ located in a secure, environmentally controlled area.
- ~~5.4.~~ The backup copy of the records shall be stored on highly-secured, immutable, backup media. The tertiary copy shall only be accessed through a gateway technology that prevents direct access to the storage media from the system(s) being backed up. Manufacturer's usage specifications and backup system media replacement guidelines shall be followed at all times, in accordance with ACJA § 1-504(G)(2).
- ~~6.5.~~ At a minimum, a ~~A~~ daily, ~~incremental~~ backup of the primary copy of records ~~added to the archive~~ shall be made using automated backup software.
6. Backups shall be stored in a secure, environmentally controlled, offsite location and retained a minimum of 28 days offsite. Full backups should be made not less than weekly and retained a minimum of 28 days offsite before reuse.
7. When any system outage occurs, all records must be available not later than the end of the tenth business day.

F. Authorization to Destroy Paper Case Records. Any court desiring to implement a paperless case record operation shall obtain advance written approval of its operational policies and EDMS infrastructure as described herein from the Administrative Office of the Courts (AOC). The AOC shall provide a form for courts to use to request approval. The form shall include a checklist of audit criteria for electronic records management practices and infrastructure.

1. through 6. [No change]
7. Authorization is not needed to destroy paper case records maintained in the central document repository supported by the AOC or other document repository approved by the Arizona Judicial Council or the Commission on Technology, provided the court complies with ~~subsections~~ paragraphs (D)(1)(c)&(d), (D)(4)(b)&(c), and (D)(5)(c) of this section and all related operational requirements of ACJA §§ 1-504 and 1-506.

G. Authorization to Destroy Paper Administrative and Regulatory Case Records. The presiding judge of the county is authorized to approve destruction of paper administrative and regulatory case records maintained by the courts under the presiding judge's supervision. The administrative director is authorized to approve destruction of paper administrative and regulatory case records maintained by the AOC. They shall ensure that the applicable standards and protocols established by ~~subsection~~ paragraph (E) have been met before approving destruction of paper records. Superior court clerks who meet the requirements of ~~subsection~~ paragraph (E) are authorized to destroy the paper administrative and regulatory records they maintain without prior approval of the presiding judge.

H. Electronic Archives of Closed Cases in Limited Jurisdiction Courts. Justice and municipal courts that wish to create an electronic archive of closed case files and destroy the corresponding paper records prior to the applicable retention and destruction date shall meet all standards and protocols ~~established by this section in paragraph (D),~~ with the following modifications:

1. Copies of the archived records can be limited to one primary copy and one backup copy. ~~The primary copy of all electronic records in the archive shall be maintained online at all times using at least one RAID Level 5 disk or storage array.~~
2. ~~The EDMS application, SQL database, and backup software for the archive may reside on internal magnetic storage in a RAID Level 1 configuration, if these applications are not stored on the RAID Level 5 disk or storage array.~~
- 3.2. On-premises sServers used for an electronic archive shall be ~~installed in a rack or other fixture~~ located in a secure, environmentally controlled area.
4. ~~The backup copy of the archive shall meet the requirements of subsection (D)(3)(e).~~
- 5.3. A daily, incremental backup of the primary copy of records added to the electronic archive shall be made using automated backup software.
- 6.4. Courts are not required to ~~comply with subsection (D)(3)(e)~~ have redundant network pathways from end-user devices to the electronic archive.
- 7.5. When any system outage occurs, all archived records must be available not later than the end of the fifth business day.