

IN THE SUPREME COURT OF THE STATE OF ARIZONA

In the Matter of:)	
)	
ARIZONA CODE OF JUDICIAL)	Administrative Order
ADMINISTRATION § 1-507:)	No. 2016 - <u>113</u>
PROTECTION OF ELECTRONIC)	(Affecting Administrative
RECORDS IN PAPERLESS COURT)	Order No. 2012-07)
OPERATIONS)	
_____)	

An amendment to the above-captioned section of the Arizona Code of Judicial Administration having come before the Arizona Judicial Council on October 27, 2016, and having been approved and recommended for adoption,

Therefore, pursuant to Article VI, Section 3, of the Arizona Constitution,

IT IS ORDERED that Arizona Code of Judicial Administration § 1-507 is amended as indicated on the attached document. All other provisions of § 1-507, as originally adopted, remain unchanged and in effect.

Dated this 2nd day of November, 2016.

SCOTT BALES
Chief Justice

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. through C. [no changes]

D. Requirements Applicable to Case Records.

1. General Requirements.

- a. Courts shall not create or store electronic records using systems that employ proprietary designs, formats, software, or media or that require use of non-standard devices to access records, in accordance with ACJA § 1-504(C)(1).
- b. Courts shall preserve all electronic documents so that the content of the original document is not altered in any way and the appearance of the document when displayed or printed closely resembles the original paper without any material alteration, in accordance with ACJA § 1-506(D)(1).
- c. Courts shall preserve evidence and fingerprints in their submitted format – hardcopy items shall not be converted to electronic records for the purpose of storage and electronically submitted items shall not be converted to hardcopy for the purpose of storage.
- d. Printouts of electronic records shall be provided to other courts, as needed, unless arrangements have been made for those courts to receive electronic documents in lieu of paper.

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 EDMS application shall reside on two physically separate servers each using separate internal storage, structured query language (SQL) databases, and backup software. Log shipping shall be employed not less than daily to maintain synchronization of the two EDMSs for disaster recovery.
- 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 ~~(E)~~ (F) of this section.

3. Storage Requirements.

- a. Courts shall maintain primary and secondary copies of records online at all times using at least two physically separate, ~~RAID Level 5, disk storage~~ arrays configured to assure the failure of a single component of the array will not impact the integrity of the data. New records shall be written simultaneously to all disk arrays.
- b. Primary and secondary storage shall be attached only to ~~dedicated~~ 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 ~~switches~~ paths to connect workstations and imaging devices to EDMS application servers.
- d. 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 backup media ~~that remains disconnected from the network unless actively creating a backup or restoring a backup using automated backup software.~~ 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(~~FG~~)(2).
- f. Backup media shall be stored in a secure, environmentally controlled, offsite location and retained a minimum of 28 days offsite before reuse. Full backups shall be made not less than weekly and retained a minimum of 28 days offsite before reuse.
- g. Backup and restoration procedures shall be documented and tested for effectiveness.
- h. Scanned records shall appear on the backup media as well as primary and secondary storage before corresponding paper is destroyed.

4. Imaging and Indexing Requirements.

- a. Scanning quality must comply with *Recommended Practices for Quality Control of Image Scanners* (ANSI/AIIM MS44-1988 (R1993)), in accordance with ACJA § 1-504(D)(~~5~~3).

- b. The EDMS shall be integrated with the CMS or the following categories of metadata (as a minimum) shall be recorded in the EDMS:
- Case number (including type code),
 - Party names,
 - Standard document type identifier,
 - Date of filing, and,
 - Citing agency number, where applicable.
- c. Index entries shall be verified to ensure records are accurately retrieved prior to destruction of any corresponding paper originals. Un-retrievable records shall be rescanned and re-indexed until they prove to be accurately retrieved from the EDMS.

5. Support and Maintenance Requirements.

- a. Court personnel or contractors ~~shall~~ must be certified in the following areas required to proficiently operate and maintain the records management system:
- (1) Microsoft Certified Systems Administrator
 - (2) Microsoft Certified ~~IT Professional~~ (≥SQL2005) Database Administrator
 - (3) OnBase Certified Advanced System Administrator or equivalent for any approved, non-conforming EDMS.
- b. When any system outage occurs, all records must be available not later than the end of the following business day. If lost, redundancy must be re-established as quickly as is practicable, even if records remain fully available in the non-redundant state.
- c. Records generated by or received by courts shall be preserved in accordance with the applicable records retention schedule. Case records required to be submitted to Arizona State Library, Archives, and Public Records (ASLAPR) shall meet the submittal requirements specified by ASLAPR at the time of submittal, regardless of storage medium. Records destruction is subject to the notification requirements of ASLAPR.
- d. In accordance with ACJA § 1-504(~~EF~~)(43), courts shall periodically refresh electronic records in order to ensure their accessibility for as long as the applicable records retention schedule requires. Refresh procedures may require recopying of files to new media or ~~disk~~ storage arrays over time.
- e. Courts shall ensure continued accessibility via a planned migration path so devices, media, and technologies used to store and retrieve records are not allowed to become obsolete and are promptly replaced or upgraded, in accordance with ACJA § 1-504(~~EF~~)(21).
- f. Courts shall ensure that any new equipment or software replacing that used in an existing system is backward compatible and shall obtain a vendor certification that

the system will convert 100 percent of the images and index data to the new system so access to existing electronic records is never impeded, in accordance with ACJA § 1-504(FF)(32).

E. Requirements Applicable to Administrative and Regulatory Case Records.

Requirements applicable to case records apply to administrative and regulatory case records with the following modifications.

1. 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. Servers used for an electronic archive shall be installed in a rack or other fixture located in a secure, environmentally controlled area.
5. The backup copy of the records shall be stored on highly-secured backup media ~~that remains disconnected from the network unless actively creating a backup or restoring a backup using automated backup software.~~ 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(FG)(2).
6. A daily, incremental backup of the primary copy of records added to the archive shall be made using automated backup software.
7. When any system outage occurs, all records must be available not later than the end of the tenth business day.

F. and G. [no changes]

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, 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. Servers 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. A daily, incremental backup of the primary copy of records added to the archive shall be made using automated backup software.
6. Courts are not required to comply with subsection (D)(3)(c).
7. When any system outage occurs, all archived records must be available not later than the end of the fifth business day.