



FLORIDA COURTS TECHNOLOGY STANDARDS
SECTION III: ELECTRONIC COURT RECORDS CUSTODIAN
[ALL-IN-ONE DOCUMENT]

{11/1/2020}

E: TextBookDiscrimination@gmail.com

W: www.TextBookDiscrimination.com

visit TBD's [website](http://www.TextBookDiscrimination.com) for the most up-to-date information

TABLE OF CONTENTS | SECTION 3: ELECTRONIC COURT RECORDS CUSTODIAN...

#	Section	Title	Page
C01	3.0.0	Section 3 Intro	4
C02	3.1.0	Court Document Format	5
C03	3.2.0	ADA Compliance	6
C04	3.3.0	Court Records Redaction	7
C05	3.4.0	Court Records Storage	8
C06	3.5.0	Court Records Backup and Archival	9
-	n/a	Appendix	10



FLORIDA COURTS TECHNOLOGY STANDARDS

SECTION: 3

CAPTION: ELECTRONIC COURT RECORDS CUSTODIAN STANDARDS

ITEMS: 3.0.0 through 3.5.0



ITEM 3.0.0 | SECTION 3 INTRO

Electronic court records custodians are responsible for the storage, processing, security, availability, accessibility, and integrity of electronic court records (i.e., images and data) under their care.

These standards are minimum standards. If a custodian stores court-related data from another jurisdiction or agency with stricter requirements, the custodian must comply with the stricter standards for that data.



ITEM 3.1.0 | COURT DOCUMENT FORMAT

Custodians shall ensure that:

- Electronic documents that are part of a court file (i.e., the record copy) are stored in the PDF/A format.
- This is a day-forward standard.
- Upon implementation of the PDF/A standard for incoming filings, existing electronic documents may remain in their current format(s) if the clerk's CMS is capable of managing multiple file formats.
- The record copy of each electronic court document retains the original document intelligence (i.e., as filed with the Portal) except features that use a digital hash. For example, digital signatures and electronic notarizations may be flattened and the certificates invalidated as the document moves through the filing process.



ITEM 3.2.0 | ADA COMPLIANCE

Custodians of electronic court documents are not responsible for adding ADA-compliance features to documents that they did not originate. However, custodians are required to follow acceptable ADA practices for access to court documents.



ITEM 3.3.0 | COURT RECORDS REDACTION

Custodians shall ensure that confidential information contained within a court record is redacted before release or review of the record as defined by Fla. R. Gen. Prac. & Jud. Admin. 2.420.

Redaction software that identifies confidential information may be used; however, a manual process must also exist to identify confidential information that may not be readily identified by an automated redaction process or for case types/documents that are available upon request. Redacted copies of electronic court documents are not required to retain the original document intelligence. These copies may be flattened to accommodate existing redaction workflow processes.



ITEM 3.4.0 | COURT RECORDS STORAGE

Custodians shall ensure that:

- All court data under their care is stored in the United States. This includes the record copy and all backup and archival copies.
- The production data or backup copy will reside in a hardened (CAT 5) facility. If a hardened (CAT 5) facility is unavailable, a tertiary copy (redundant backup) will also be maintained in its own offsite, independent facility. The production of electronic court records and at least one copy of the backup(s) shall not be housed in the same building.
- Agreements with third-party vendors for cloud or offsite copies acknowledge the confidentiality of electronic court data they store and prohibit data mining and other access/use of the data for any purpose other than to make the data accessible to the custodian.
- All copies of court data must be readily available to the custodian.
- Any known breach, or other malicious events, is reported to the chief judge or his/her designee and the Chief Information Security Officer at the Office of the State Courts Administrator Office of Information Technology as part of the custodian's Computer Security Incident Response plan.
- Physical and electronic data transfer processes conform to the confidentiality and security guidelines outlined in Section 7, Data Exchange.



ITEM 3.5.0 | COURT RECORDS BACKUP AND ARCHIVAL

Custodians shall ensure that:

- Electronic court records in their care are securely backed-up and any backup data stored at a third-party location must also be encrypted. The custodian of the electronic court records shall have exclusive access to the encryption key. In instances where vendors are supporting appliances onsite and are required to maintain an encryption key, the custodian will have operational policies and procedures that serve as a control prohibiting vendor access without invitation and monitoring.
- Random sample testing is performed annually to verify that backup data is accessible and recoverable.
- Archival copies are created in a manner that allows for presenting the information in the future without degradation, loss of content, or issues with software compatibility relative to the proper rendering of electronic documents.



APPENDIX



COPYRIGHT NOTICE

TextBookDiscrimination.com is not the author of these rules. Instead, TextBookDiscrimination.com merely re-printed and reformatted them for easier use.

ORIGINAL SOURCE

<u>#</u>	<u>Item</u>	<u>Link</u>
1	Original Source	www.FLCourts.org

CONTACT INFORMATION

E: TextBookDiscrimination@gmail.com

W: www.TextBookDiscrimination.com

Congratulations! You're now ***booked up*** on Section III (*Electronic Court Records Custodian*) of the Florida Courts Technology Standards!

