FCTC

Action Summary

August 2017

- FCTC approved the following motion for first reading: Motion to require the Portal E-Filing Authority to schedule maintenance so that the conclusion will occur on the same day as the commencement. For instance, a 5-hour scheduled maintenance should begin no later than 6 PM. Ideally, scheduled maintenance begin shortly after midnight.
- FCTC approved the following motion for second reading: Motion to recommend to the Supreme Court that judicial officers file and serve their orders through electronic means by September 1, 2018.
- FCTC approved the following motion for second reading from the FCTC/RJA Joint Workgroup: Motion to delete standard 3.5.3 Original Documents or Handwritten Signatures in the *Standards for Electronic Access to the Courts*, which states "Original documents, such as death certificates, or those that contain original signatures such as affidavits, deeds, mortgages and wills must be filed manually until further standards have been adopted.
- FCTC approved the following motion for first reading from the Technical Standards Subcommittee: Motion to recommend approval of the Backup of Electronic Records language.

Backup of Electronic Records

Court records custodians are responsible for the security, availability, and integrity of electronic court records under their care. Therefore, these custodians shall ensure that:

- Electronic court records in their care are securely backed-up and are recoverable.
- Data and systems backups are stored in a protected environment that is off site from the primary storage location of the court record, and at a certified hardened facility based on FEMA, GSA or other applicable building standards.
- Third party offsite backup vendors comply with applicable Florida Supreme Court Technology Standards.

- Agreements with third party offsite vendors 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.
- The custodian shall not allow court data backups to be stored, encrypted, manipulated or otherwise rendered unavailable without the ability to access the backups using industry standard technology.
- Random sample testing is performed annually to verify that data is accessible and recoverable.
- Any known breach, or other malicious event, 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.
- All court backup data is stored in the United States.
- Physical and electronic data transfer processes conform to the confidentiality and security guidelines set forth in the Data Exchange Standards.

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.