

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.

