

ITEM 2.2.13 | SYSTEM AVAILABILITY AND RECOVERY PLANNING - PLANS

2.2.13.1 Plan 1: Contingency Plan

Timeframe: Immediate - during normal working hours.

Scope: Localized system failures while court is still open and operational. This plan will also be put into operation when Continuity of Operations ("COOP") and Disaster Plans are implemented.

Operational Levels: Levels of operation will be temporarily limited and may be conducted in electronic or manual processes. Since court will still be open, this plan must address how documents will be received while the system is down.

Objectives:

- Allow the court to continue with minimum delays by providing a temporary alternate solution for access to court files.
- Conduct tests to verify the restoration process.
- Have local and local offsite backup of the operating system, application software, and user data available for immediate recovery operations.
- Identify areas where redundancy is required to reduce downtime and provide for "hot" standby equipment that can be utilized in the event the Contingency Plan is activated.

2.2.13.2 Plan 2: Business Continuity/Disaster Recovery

Timeframe: Disaster dependent, varies.

Scope: Declared disasters either local or regional that impact the geographic area.

Operational Levels: Temporarily unavailable or limited until facilities are deemed functional or alternate facilities can be established. Mission Essential Functions as defined in the Supreme Court's COOP for the affected area must be addressed in the designated priorities and timeframes.



Objectives:

- Allow court operations to recover in the existing location or alternate facility.
- Provide cooperative efforts with impacted entities to establish access to court files and allow for the continuance of court proceedings.
- Provide in the Contingency Plan a temporary method to meet or exceed Mission Essential Functions identified in the Supreme Court's COOP.
- Provide another tier level of recoverability by having a backup copy of the operating system, application software, and user data in a protected environment outside of the local area not subject to the same risks as the primary location for purposes of recovery according to standards approved by the FCTC.
- This plan may provide another out-of-state tier for data backup provided that the non-local in-state tier is established.

