MEASURES FOR JUSTICE

Data Repository Best Practices

We have outlined the key capabilities a state agency should have when serving as a criminal justice data aggregator and repository, offering guidance to help you identify the right resources and structures needed to support this critical work across the state.

MEASURES FOR JUSTICE

Data Repository Best Practices

MFJ recommends that each state designate a state agency to serve as a criminal justice data aggregator and repository, with the specific agency varying based on state dynamics and criminal justice structures.

Below are a set of capabilities that a data aggregator and repository agency should have:

- ☑ Uses open web standards. Little use of proprietary technology.
- ☑ Uses security on the transport layer. Website is https (rather than http) even for non-login pages.
- ☑ Uses modern scaling technologies (Tech that allows you to handle large spikes in traffic).
- ☑ Has people on staff that are dedicated to web user-interface coding.
- ☑ Has people on staff that are dedicated to web service ("server-side") coding.
- ☑ Makes data available in machine-readable, open format files (i.e., you can get full datasets without scraping).
- ☑ Makes data available and searchable via modern web APIs (access to data directly through programs, not just by humans going to web pages).
- ☑ Has the capability to aggregate, stitch together and validate the data coming in.
- ☑ Can handle, for example, duplicate, overlapping or missing data and has processes for the rejection and re-transmission of invalid data.
- ☑ Uses standard best practices for data protection and redundancy (remote backups, logging, event detection). If you're interested in MFJ assessing your state's data or want to know more about how to improve data collection, recording, and sharing, please contact us.