



◆ INDUSTRY OVERVIEW / PUBLIC SAFETY

How Verillian helps drive **compliant adoption of frontier AI** for public safety

CJIS Security Policy v6.1



Officers, analysts, dispatch staff, and records teams can use AI to draft reports, summarize case material, and search for patterns. Criminal-justice data still demands strict handling, so adoption needs a control that acts before the data crosses the boundary. **Verillian is self-hosted in your environment and aligned to CJIS Security Policy v6.1. It governs what AI may do with criminal-justice data on the device, blocks what policy forbids, and seals each captured interaction into a tamper-evident record your agency holds.**

WHAT THE READER CAN EVALUATE

GOVERN AI ON CRIMINAL-JUSTICE DATA

Tool calls on the Anthropic API format are decided on the device against deny-by-default policy before they run; other captured calls are recorded.

REDACT BEFORE A CALL LEAVES

Sensitive identifiers are stripped in place on a best-effort basis before a request reaches a model provider.

KEEP THE RECORD IN AGENCY HANDS

Each captured interaction is signed and hash-chained, sealed under a key only your agency can read.

CONTAIN FAST WHEN NEEDED

Cut off AI across the fleet at connect time with a single confirmation, and land the containment action in the record.

The record

Aligned to CJIS Security Policy v6.1 for handling criminal-justice information, not certified against it. Your agency holds the authorization. Verillian provides the on-device controls and the record.

Use this brief to frame a pilot around AI adoption, policy enforcement, and evidence your team holds.

Verillian is self-hosted with customer-held keys and tamper-evident records.

verillian.ai/industries/public-safety/