

The Most **Secure, Confidential** **Trusted** Intelligence Platform



We do not train shared AI models on department data, and conversations with TruAssist auto-delete after every shift — protecting the privacy of officers and community members alike.

| Security & Compliance

- **FBI CJIS Security Policy v6.1** — Independently audited by the Arizona Department of Public Safety and TX-RAMP certified
- **SOC 2 Type II Certified** — Independently verified controls for security, availability, and confidentiality over a sustained period, not just a point-in-time review.
- **100% AWS GovCloud** — All infrastructure runs in AWS GovCloud. TRULEO refuses to run on Microsoft Azure.
- **MFA / SSO / RBAC** — SAML and Microsoft Entra ID support for single sign-on, required multi-factor authentication, and role-based access control (RBAC) — matching agency IT security policy.

| Confidentiality & Privacy

- **100% Confidential** — Conversations with TruAssist auto-delete after every shift (12 hours), and generated reports are retained for 60 days — long enough to be useful, short enough that we don't hoard your data.
- **100% Made in the USA** — Every developer and support staff member who touches TRULEO is a U.S. citizen working on U.S. soil. No offshore engineering, no foreign-support workaround, no ambiguity about who can see agency data.
- **IPS 140-3 Validated Encryption** — All data is encrypted in transit and at rest using FIPS 140-3 validated encryption, meeting the federal bar for sensitive government data.
- **Read-Only, Agency-Controlled Access** — TRULEO connects to RMS, BWC, and jail call platforms via secure, pre-built, read-only connectors — agencies control what's shared and can revoke access at any time.

| Independently Validated by Academic Research

TRULEO opens itself up to randomized controlled trial (RCT) studies with leading criminologists around the country — Clemson University, the University of South Carolina, and Arizona State University — independent research that found TRULEO improves outcomes for both officers and the community members they serve.

| We Protect Both Officer & Community Privacy

- **Personal Info Auto-Redaction** — Names, addresses, plates & IDs redacted from BWC transcripts automatically.
- **No BWC Surveillance Search** — No global search across transcripts — independently audited.
- **We Reject Surveillance Use Cases** — We decline features that enable population monitoring instead of case-tied investigation.

Quick Stats

1,000+
agencies nationwide

Zero data security incidents —
never breached, never leaked

SOC 2 Type II
certified

FIPS 140-3
encryption standard

AWS GovCloud
hosting environment

Compliance logos aren't enough.

Here's what agencies are asking — and how TRULEO answers.

Have you ever experienced a data breach or unauthorized disclosure?

No. TRULEO has never experienced a data security incident or unauthorized disclosure of department data.

Where is your infrastructure hosted?

100% AWS GovCloud — a government-authorized environment purpose-built for sensitive, regulated workloads. TRULEO does not use Microsoft Azure or any general-purpose commercial cloud.

Are any developers or support staff located outside the United States?

No. 100% of TRULEO's development and support team are U.S. citizens working on U.S. soil. There is no offshore engineering team — offshoring is a practice we consider despicable in U.S. public safety.

Can every person who touches our data pass a CJIS fingerprint background check?

Yes. Personnel screening aligns with the FBI CJIS Security Policy's requirements for anyone with access to Criminal Justice Information.

Is your CJIS compliance independently verified?

Yes. TRULEO was recently audited by the Arizona Department of Public Safety.

How does TRULEO access our systems?

Via secure, pre-built, read-only connectors to RMS, BWC, and jail call platforms.

You provide us credentials — no expensive vendor API contracts required.

How long do you retain our data?

Conversations with TruAssist are stored for 12 hours and auto-delete. Reports your officers create are stored for 60 days. TRULEO never stores BWC video for analysis — it streams from your evidence platform and stores only the analysis. That analysis auto-deletes after 60 days.

Do you use our data to train your AI models?

No. Department data is never used to train shared AI models. TruAssist operates on a closed-loop, CJIS-compliant knowledge base — fundamentally different from querying a public LLM like ChatGPT. We also have Zero Data Retention agreements with OpenAI and Anthropic.

Do you save our conversations with TruAssist?

Conversations with TruAssist are saved for only one shift (12 hours) — protecting the privacy of both officers and the community members referenced in a case.

What authentication does TRULEO support?

MFA and SSO via SAML and Microsoft Entra ID — matching the identity and access management your IT team already runs.

Will you put your answers in writing?

Yes. TRULEO will answer all of the above in writing, with audit documentation to back it up, at truleo.co/security or on request from your account team.

Downloadable Audit Documentation (truleo.co/security)