

TECHNICAL — DATA PROTECTION

How ARGUS Protects Information

ARGUS is built on a layered protection model. This paper explains the model in plain terms — enough to evaluate it with confidence, without disclosing implementation specifics.

Layer 1 — In transit: the translation table

Before any lookup leaves the device, sensitive values are replaced with generic, typed placeholders using a per-session mapping table. What crosses the network carries **no plaintext identities** — names, addresses, and other sensitive fields are represented only as neutral tokens. The real values are restored only locally, for the authorized operator.

Layer 2 — At rest: encryption

Stored sessions are **encrypted with AES-GCM-256** using hardened key derivation. On disk, an entry is a non-identifying stub — no readable coordinates, agenda, or names. Recall decrypts only with the correct key; a wrong or absent key **fails safe** to a "Protected session" placeholder rather than exposing anything.

The decrypt key lives in a different layer

The key that makes data legible is the operator's access grant, held separately from the data itself. So even if a stored record were reached and one layer were decrypted, without the mapping table and the grant key the result is illegible tokens — not readable intelligence. Legibility requires both layers, held apart.

Access control

- › **Invitation-only** — no public sign-up; access is issued and can be revoked instantly.
- › **ID plus one-time code** — the code is stored only as a hash, never in the clear; the readable ID alone is never the key.
- › **Client PII stays in the secured cloud database** — never in shared files or working documents.
- › **Team-controlled** — a team lead governs who has access and at what permission level.

AI handling

Assessments are generated by a leading enterprise AI model through a server-side gateway. The AI credential **never reaches the device**, and the queries sent for analysis are de-identified by the Layer-1 translation table.

What we do not do

We do not expose the "how." The tool never asks an operator to type keys or credentials into a page. There is no public listing and no app-store distribution — access is by invitation only. The confidential implementation of each protection lives in a separate, privileged document.

Informational use only. Analysis is machine-generated from publicly available and open-source information and must be verified before operational use. ARGUS is not a substitute for licensed security, legal, or medical professionals, or for emergency services — in any emergency, call 911.