

VERITROOPER Scout — Data Handling & Isolation Posture



Generated — OSHA_29CFR_full_2024 — veritrooper v9
13 July 2026

For the audit of Meta-Llama-3.1-70B-Instruct. Generated 2026-07-13 23:17:27.

This document records the data-handling facts of this audit run and the network mode it can and cannot establish. It complements — it does not replace — your own network controls and any accreditation (e.g. ATO, FedRAMP, DoD IL). It is not a cryptographic attestation and does not certify the audited system.

Verifiable data handling

- **Read-only over source & model.** The engine reads the evaluated material and queries the model; it does not modify or export either.
- **Local artifacts only.** The only data written is this audit's own output (reports, JSON, this document), written locally into the results folder you control. It is not transmitted anywhere by the engine.
- **Bundled local grader available.** VERITROOPER ships an offline validator, so the grading step can run with no third-party judge model.

Components recorded for this run

Role	Recorded as	Locality
Model under test	Meta-Llama-3.1-70B-Instruct	endpoint locality not captured — confirm on your network
Verification model (Doctor)	Meta-Llama-3.1-70B-Instruct	endpoint locality not captured — confirm on your network
Independent verifier	GPT (frontier model)	endpoint locality not captured — confirm on your network

Network mode

Overall network isolation is **determined by the endpoints the operator selected** for the model under test and the Doctor. When every selected endpoint is on your network or local, the whole audit runs with no outbound internet; when a hosted API is selected, that component reaches out. This record does not capture each endpoint's address, so it does not assert full air-gap on its own — confirm the mode with your network monitoring (or a pre-run isolation check) for a demonstrable attestation.

What this is NOT

- Not an accreditation (ATO / FedRAMP / DoD IL) — that is the operating environment's, not this tool's.
- Not a cryptographic boundary or a zero-bytes-written claim — the engine writes its own audit artifacts locally.
- Not a certification of the audited system's security or conformity.

Framework relevance

Supports data-minimization and system-boundary considerations under the NIST AI RMF and data-handling controls under ISO/IEC 42001; confirm the specific controls against your own control set.

Contents (click a section to jump)

Verifiable data handling

Components recorded for this run

Network mode

What this is NOT

Framework relevance

Generated by VERITROOPER as a data-handling & isolation posture record. This artifact is testing evidence only. It does not by itself constitute, certify, or confer conformity with any framework, and does not replace the conformity assessment or the provider's other obligations. Have counsel review before external use.