idsideAI v6.0 — Verification Checklist

Date: 2025-08-26

A) Integrity & Provenance

- Download the three artifacts: Gold v6.0 R1, App v6.0, Checksums.
- Verify SHA-256 of the audit pack: compare idsideAI_v6_0_Audit_DETAILED_SHA256.txt to local hashes.
- Open Gold zip → confirm /idsideAIfinal_PyCharm_Ready/INTEGRITY contains: DETAILED audit PDF, DETAILED matrix CSV, SHA file, manifests.

B) Environment Setup

- Unzip idsideAI_App_v6_0_FINAL_PyCharmReady.zip
- cd idsideAIfinal_PyCharm_Ready
- python -m venv .venv && source .venv/bin/activate (Windows: .venv\Scripts\activate)
- pip install -r requirements.txt
- python -c "from app.utils.db import init_db; init_db()"

C) Static Sanity (no server)

- Compile all .py: python - <<'PY'\nimport os,py_compile;import sys root='.' errs=0 for dp,_,fs in os.walk(root): for fn in fs: if fn.endswith('.py') and not fn.endswith('.py.disabled'): p=os.path.join(dp,fn) try: py_compile.compile(p, doraise=True) except Exception as e: print('ERR',p,e); errs+=1 sys.exit(1 if errs else 0) PY
- Optional: flake8/pylint and bandit (if available).

D) Run Server

- uvicorn app.main:app --reload
- Open http://127.0.0.1:8000/ (or the printed host/port).

E) Unified Run Flow (/run)

- Open /run. Enter a simple prompt. Submit in Standard mode → expect JSON with {mode, provider, model, latency_ms, quality, text}.
- Switch to Turbo → expect higher quality and potentially higher latency; response payload includes same fields.

F) Decision Models

- POST /decision-models to create (or use UI flows if available).
- GET /decision-models → verify listing, search (q), tag filter (tag).
- GET /decision-models/{id} → verify full record with parsed graph.

- Open /decision-models/view?id={id} → SVG graph renders nodes/edges; Raw JSON matches store.
- GET /decision-models/{id}/export?fmt=json|csv|pdf → verify downloads open and content is correct.

G) Settings (BYO API Keys)

- Open /settings → save an API key for a provider (e.g., OpenAI).
- GET /settings/keys → verify provider listed with created_at.
- Security note: confirm key is not echoed back in clear; values masked in UI (design choice).

H) Sharing / Roles

- POST /share with { dm_id, email, role } → expect record created.
- GET /share/{dm_id} → verify list includes your entry.
- NOTE: Access enforcement on DM endpoints is intentionally not wired; confirm this limitation is documented in the audit.

I) Telemetry

- Trigger several /run calls (Standard and Turbo).
- Open /telemetry → confirm charts update for latency and quality.

J) Security & Ops

- Use curl -I against any route and verify headers: X-Frame-Options=DENY; X-Content-Type-Options=nosniff; Referrer-Policy=same-origin.
- Rate limit: hammer a route >50x within 10s from same IP → expect HTTP 429.

K) Tests

- pytest -q
- Expect core tests (run, decision models, graph utils) to pass. Investigate failures, if any.

L) Acceptance Summary (Board Proof)

- Confirm all items A–K pass.
- Attach the DETAILED Audit PDF and Matrix CSV with SHA-256 to your verification report.
- State clearly: App matches business-plan requirements; app is integrated, pyCharm-ready, and verifiable.