Atlas Technical Brief — Privacy, Controls, and Pilot Readiness (v1.0)

Purpose

Outline the architecture, privacy model, safety controls, and partner-facing assurances for Atlas (healthy-exercise → proof-of-effort tokens). Code is not included; detailed math/governance exist and can be shared later under NDA.

1) Architecture & Data Flow

- **Device (phone/watch):** collects motion/heart-rate signals; performs **on-device feature extraction**; runs liveness/safety checks.
- **Proofs-not-data:** device emits a **verifiable attestation** (e.g., zero-knowledge style predicate: "safe activity ≥ threshold; tests passed"), never raw streams.
- **Transport:** mutual-TLS; request includes **idempotency key** (pseudonymous user_id, window id, nonce, feature hash).
- **Server:** validates proof, applies **non-punitive policies**, mints a token, writes audit logs.
- **Ledger/Treasury:** accounting only; no personal data.

[Watch/Phone sensors] → On-device analysis → ZK-style attestation → TLS → [Server validates] → Mint token → Ledger

2) Privacy & Security Model

- **Data minimization:** No raw motion/biometric data leaves device; only bounded summaries/proofs.
- **Pseudonymity:** Server uses a stable pseudonymous user_id; partners do not receive raw IDs.
- **Idempotency & replay safety:** Each event has a unique key; duplicates do not mint twice.
- **Retention:** Raw features remain on device only (short window, e.g., ≤24h). Server stores proofs + minimal metadata.

- **Governance:** Parameter changes time-locked; configurations auditable.

3) Safety & Accessibility Controls

- **Health safety:** session caps, cool-downs, accessibility carve-outs; human override by partner staff.
- **Non-punitive guarantee:** Penalties/multipliers **never** touch guaranteed benefits (if present).
- **Fairness floors:** Allow-listed venues and accessibility flags receive soft floors to prevent inadvertent under-rewarding.
- **Anti-gaming:** anomaly/outlier filters; randomized audits; co-location heuristics with venue allow-lists.

4) Tokens & Incentives (Loyalty-Style)

- Tokens function like **loyalty points** for healthy behaviour; partners map them to **small, practical perks** (transit, groceries, fitness) under their policies.
- No speculation or financial exposure is required for partners.

5) Compliance Posture (Plain Language)

- **Consent:** Opt-in only; plain-language participant info; withdrawal at any time without consequences.
- **Privacy (PIPEDA principles):** purpose limitation, data minimization, safeguards, individual access (through partner).
- **Financial/consumer:** Tokens are for **evaluation**; any redemption is loyalty-style and partner-controlled.
- **Public communications:** No publicity without mutual consent.

6) What a Pilot Would Look Like (Informational)

- **Scope:** limited, opt-in cohort; isolated devices/network if preferred; no client identifiers required.
- **Measures:** engagement minutes, routine completion, attendance/retention, optional well-being check-ins.

- **Artifacts we can provide:** consent template, DPIA outline, technical controls checklist, daily/weekly activity summaries (aggregate).

7) Status & Next Step

- Documentation/governance/math are complete; **system is ready for pilot** pending partner fit and ethics review.
- We propose a **brief meeting** to discuss alignment; if interested, we'll provide the private repo and detailed appendices **under NDA**.

draunali@renaissance-ecosystem.com