



JUDGEMENT SPINE

Security Model - Data Handling & Redaction (Public)

How to make proof portable without leaking sensitive data.

Data minimisation

- Store identifiers and hashes in the evidence pack; store raw sensitive payloads in existing secure systems.
- Redact secrets and credentials by default.
- Prefer references to ticket IDs, telemetry IDs, object store paths (with access controls).

PII guidance

- Do not embed full customer records inside packs unless explicitly required.
- If needed, use field-level redaction and access controls.
- Record purpose codes and approvals for any export of regulated data.

Retention

- Retain packs in line with incident response and regulatory timeframes.
- Separate storage tiers: hot (incident), warm (audit), cold (archive).

Contact: founder@judgementspine.com