SaaS AI Trust Pack

Make AI features enterprise-ready: proof buyers trust and reviewers approve.

Why this matters now

- Regulated buyers (FS/EU) increasingly expect clear assurances for AI features: BYOK/customer-managed keys, deeper audit logging (prompt/model I/O), and regional data residency options.
- Executives fund security that enables revenue: shorten DDQs, reduce escalations, and give Sales a clear, repeatable set of buyer-grade proofs.

What's in the pack (deliverables)

- AI System Card: purpose, inputs/outputs, supported uses/limits, data classes (PII/PHI) and minimization strategy.
- Data-flow & lineage diagram: prompt/context ingestion, model/tooling calls, caches/stores, retention, and access boundaries.
- Logging for reviewers: searchable prompt/response logs, admin access logs, evaluation run logs; exportable on request.
- Safety & evaluation: red-team scenarios (jailbreak/PII leakage), offline evals, risk acceptance/mitigation register (top 10).
- Policy excerpts: AI Acceptable Use, developer guardrails, shadow-AI intake/procurement, model update/change-control.
- Buyer assurances letter & FAQ: BYOK options/roadmap, logging depth, residency posture, DSAR/erasure process, subprocessors.
- Control mapping: SOC 2, ISO 27001 control references; NIST AI RMF alignment notes (v1.0).

Outcomes & KPIs we target

- DDQ/assessment turnaround: 3–5 business days for common questionnaires.
- Escalations per deal: lower and earlier resolution; fewer eng-hours pulled into reviews.
- Auditability: demonstrable logs for prompts/model outputs and admin actions.
- CFO view: one-pager showing cost vs. expected pipeline lift; invest where expected loss > control cost.

2-Week pilot (low-lift)

- Discovery: current AI features + top reviewer questions from recent deals.
- Draft Trust Pack v0.9: system card, data-flow, log samples, buyer FAQ, and control mapping.
- Board/CFO one-pager + remediation plan with quick wins for BYOK/logging/residency posture.

Compatibility

- SOC 2 (TSC) / ISO 27001 control cross-walk · NIST AI RMF 1.0 alignment notes.
- Designed for FS-facing, enterprise, and EU buyers; clean language for legal/procurement.

Contact

Tim Kiely, CISSP — Founder & vCISO, ProofPath Security
Email: tim@proofpath.com • Phone: (802) 458-7656 (ET)
Book 15 minutes: https://cal.com/tim-kiely/intro

Notes: We provide security guidance; not legal advice. AI use is opt-in and logged. Subprocessors on request.