

Version 2026-09. Prepared for client procurement and vendor-risk teams. Answers in Part A are Thinkscoop's standing commitments as published at thinkscoopinc.com/trust. Part B lists the control evidence we provide under NDA during onboarding. Average vendor onboarding is 5 business days.

PART A: STANDING ANSWERS

1. Company

QUESTION	ANSWER
Legal name and form	Thinkscoop Technologies LLP, India
Headquarters	40C, Aero Arcade, G-Block, Aerocity, Mohali, Punjab 140603, India
Founded	2017
Offices outside India	None. Team based in India; clients across the United States, Australia and the UAE
Security contact	Krishan Saini, Founder and CEO, krishan@thinkscoopinc.com , +91 7888558392
Services in scope	Software engineering, AI engineering (LLM applications, RAG, agents), enterprise platform work (Microsoft Dynamics 365, Salesforce, SAP, Power BI), staff augmentation and dedicated teams

2. Certifications and audits

Question	Answer
SOC 2	Type I audit in progress across the security, availability and confidentiality trust service criteria. Controls in scope: access management, encryption at rest and in transit, incident response, vendor risk, change management and employee security training. The report is shared with prospective clients under NDA once the audit is complete. We do not claim certifications we have not earned.
ISO 27001	Not certified. Systems and processes are designed to ISO 27001 practices.
GDPR	Systems built to comply with GDPR for clients with EU operations or customers: consent management, DSAR handling, right to erasure, data minimisation, privacy by design on new builds.
Sector frameworks	We design to and work within client requirements for HIPAA, FCA and PCI-DSS, with the client's compliance team from day one.

3. Data handling

Question	Answer
Where is client data processed?	Inside the client's own cloud environment and security perimeter: the client's VPC, cloud accounts and access controls. Nothing leaves the perimeter unless the client's architecture requires it and approves it in writing.
Is client data used to train models?	No. Client data is never used to train third-party models.
Personal data and LLMs	PII is detected and redacted before any LLM processing.
Data retention	Agreed per engagement and enforced automatically.
Data location and residency	Determined by the client's environment; we do not copy client data to Thinkscoop systems by default.
Access to client systems	Named individuals only, least privilege, provisioned and revoked by the client or under the client's process.

4. Application and AI security

Question	Answer
Secure development	Security review on every production deployment. OWASP Top 10 and dependency scanning in CI/CD.
Penetration testing	Third-party penetration testing supported, with remediation within agreed SLAs.
AI-specific testing	Prompt-injection and adversarial testing on all deployed agents and LLM applications.
AI operations	Every AI system ships with an evaluation framework, monitoring, confidence scoring, human escalation paths and full audit trails. Hallucination and accuracy service levels enforced where defined. Hard LLM spending limits with automatic circuit breakers.
Change management	Weekly staging deploys, documented handoffs, client review before production.

5. People

Question	Answer
Background verification	Every engineer, employee or contract specialist, is background-verified before touching client systems.
Confidentiality	Every engineer is under NDA before access.
Security training	Employee security training is a control in the SOC 2 Type I scope.
Subcontracting	Delivery is by a core team plus contract specialists engaged directly by Thinkscoop under NDA. Thinkscoop is the single contracting party and is accountable for all delivery. Contract specialists are disclosed where a client program asks.
Offboarding	Access revoked on the day an engineer leaves an engagement; documented handover on replacement.

6. Legal and commercial

Question	Answer
NDA	Mutual NDA signed before the first technical conversation, executed within 24 hours. Client-provided NDAs accommodated. Covers project details, architecture, business strategy, client data and proprietary processes.
Intellectual property	100% IP transfer on every engagement. Code lives in the client's repository from day one. No license lock-in, no proprietary frameworks; open-source tools and standard infrastructure. IP assignment clauses standard in our contracts.
Insurance	Certificates of insurance provided during onboarding.
Contract terms	Detailed statement of work with total cost before work begins. Exit clauses in every contract; the client owns all work produced to date.
Tax	Foreign entity; W-8BEN-E provided on request. Invoicing in USD.

7. Thinkscoop's own systems (the website and lead handling)

Question	Answer
Subprocessors for thinkscoopinc.com	MongoDB Atlas (lead submissions, hosted in the US), PostHog (product analytics, US), Brevo (email, EU), Google Analytics 4, Vercel (hosting). Listed in the privacy policy at thinkscoopinc.com/legal/privacy .
Cookie consent	No analytics data collected before consent.

PART B: EVIDENCE PROVIDED UNDER NDA DURING ONBOARDING

Available within 5 business days of a signed NDA:

1. SOC 2 Type I status letter from the auditor, and the report when issued.
2. Information security policy set (access control, encryption, incident response, vendor risk, change management, acceptable use).
3. Architecture diagrams and data-flow documentation for the proposed engagement.
4. AI risk register template and the evaluation framework description.
5. Incident response plan summary and notification commitments.

6. Business continuity and backup approach for engagement artefacts.
7. Background-verification process description.
8. Certificates of insurance.
9. Sample statement of work, mutual NDA and IP assignment clauses.
10. Named security contact and escalation path.

Requests: krishan@thinkscoopinc.com. Trust page: thinkscoopinc.com/trust.