Investor Memorandum
Confidential – For Investor Review Only

Secode™- Clean AI Security

Stage: Proof of Concept Completed | Funding: Bootstrapped

1. Executive Summary

Secode™ is the world's first Pre-MLOps AI Security Platform, securing AI systems before they are built. AI failures such as hallucination, bias, privacy breaches, insecure code, and harmful datasets originate during the development process—not in production. Today's AI safety market focuses almost entirely on runtime guardrails, model firewalls, and post-deployment monitoring.

Secode™ introduces a new category: AI safety at the point of creation.

By integrating directly into the developer's workflow, Secode™ enforces safety, security, fairness, privacy, and compliance **as code, prompts, and datasets are being created**—preventing unsafe artifacts from ever entering the MLOps pipeline.

This memorandum outlines the market opportunity, product strategy, competitive position, team capability, and proposed investment structure.

2. Problem Statement

As enterprises accelerate AI adoption, they face increasing risks:

- Hallucinations → leading to financial, legal, and reputational loss
- Bias and fairness issues → regulatory penalties & discrimination risks
- Privacy/PII leaks → violations under DPDP, GDPR, HIPAA
- Insecure code → opens attack vectors within AI agents and pipelines
- Malicious/trapped datasets → compromise downstream models
- Lack of compliance traceability → regulatory nonconformity

Yet all mainstream AI safety tools activate after deployment or late in the MLOps lifecycle.

Current Industry Gap

✓ MLOps tools validate after training
✓ Guardrails defend after inference
✓ Monitoring tools alert after misuse

✗ **Nothing protects AI during creation** — where 70% of AI risks actually originate.

The AI industry is missing the "DevSecOps for AI" layer.

3. The Solution: Secode™

Secode™ is a Secure Vibe Code Generator and Pre-MLOps AI Security Platform that enforces trusted AI development at the source.

How Secode™ Works

Secode™ plugs directly into:

- Developer IDEs
- Prompt-building environments
- Data-pipeline creation tools
- Model experimentation interfaces

It applies real-time checks for:

- **Hallucination prevention**
- **Bias and fairness scoring**
- **Prompt security & injection resistance**
- **Dataset anomaly detection & sanitization**
- **Secure code generation**
- **Compliance automation (ISO 42001, NIST AI, DPDP, GDPR)**
- **Governance & audit trails**

Key Value Proposition

“Secode™ prevents unsafe AI before it is built.”

This makes it:

- Preventive instead of corrective
- Scalable instead of reactive
- Compliance-ready by design

4. Product Overview

Core Components

1. Secode™ IDE Plug-in (Developer Integration)

- Safe prompt generation
- Secure code enforcement
- Hallucination scoring
- Real-time guardrails while coding

2. Dataset Guardian™

- Detects malicious or biased datasets
- Identifies poisoning attempts
- Enforces integrity before training

3. Compliance Engine

- ISO 42001 AI Management
- NIST AI Risk Management
- DPDP / GDPR privacy enforcement
- Auto-generated documentation & audit logs

4. Governance Dashboard

- AI risk register
- Compliance scoring
- Development audit trails
- Enterprise control center

5. Technology & Architecture

Secode™ is built on:

- Hybrid rule-based + LLM-driven safety engines
- Static and dynamic code analysis
- Prompt pattern recognition and injection detection
- Dataset anomaly detection
- Multi-policy compliance mapping
- Plugin architecture compatible with VS Code, JetBrains, Jupyter, etc.

The architecture is modular and built for enterprise expansion, including on-premise deployments.

6. Market Opportunity

AI development is accelerating globally:

- 20M+ AI/ML developers (growing ~18% YoY)
- Enterprises shifting to generative AI workflows
- Global AI regulations becoming mandatory

TAM (Total Addressable Market): $12.5B

AI developers, AI-first enterprises, regulated industries

SAM (Serviceable Available Market): $3.4B

Fintech, healthcare, autonomous systems, defense, GovTech

SOM (Serviceable Obtainable Market): $150M in 3–5 years

5,000 enterprises → 500,000 developers

Zero direct competitors in the Pre-MLOps category

Market Timing

- ISO 42001 released globally
- EU AI Act phased rollout
- India DPDP Act in force
- USA NIST AI RMF adopted widely

The timing for Secode™ is ideal.

7. Competitive Landscape

Category	Companies	Gap
Runtime AI Safety	Guardrails, Shielding, LLM firewalls	Protect after deployment
MLOps Safety	Weights & Biases, TruEra, Arthur	Validate models post-training
Data Scanning	Snorkel, Cleanlab	Limited to dataset quality
DevSecOps Tools	Snyk, GitGuardian	Not AI-specific
Pre-MLOps AI Safety	**None**	**Secode™ is first mover**

Secode™ is the only product securing AI before creation.

This gives Secode™ a defensible early-mover advantage and category ownership strategy.

8. Business Model

SaaS + Enterprise Licensing

Revenue Stream	Price
Developer Seat	$75 per user/month
Enterprise License(200+ seats)	$60k–$150k/year
Compliance Add-Ons	$20k/year
Dataset Guardian Pro	$30k/year
On-Premise Deployment	Starting $120k/year
Professional Services	$200/hour

Projected Revenue Mix (Year 3)

- 65% recurring SaaS
- 25% enterprise licensing
- 10% compliance services

High predictability & enterprise appeal.

9. Go-To-Market Strategy

Phase 1: Developer First

- Freemium version
- Plug-in marketplace distribution
- Developer communities & hackathons

Phase 2: Enterprise Sales

- Fintech, health, GovTech, AI agencies
- Compliance-driven mandates
- Partner with MLOps and cloud vendors

Phase 3: Ecosystem Integration

- Full AI Safety Control Center
- Compatibility with LLMOps/MLOps platforms
- Expansion into autonomous & multi-agent systems

10. Traction & Validation

- Proof of Concept completed
- Working plug-in + dataset engine
- Early pilots lined up
- Positive feedback from regulated-sector CIOs
- Bootstrapped progress → high capital efficiency

11. Team

The founding team of Secode™

Ramesh Bhandari, Founder

Ramesh Bhandari is a serial entrepreneur with a strong track record of building and scaling technology-driven ventures across Nepal and the United States. He is the founder of multiple companies, including IOXET Labs (software and product engineering), Growstart (a venture ecosystem platform connecting founders, investors, and lenders), Mato Agro Inc. (USA), and Lumvini LLC. With deep experience in product strategy, business modeling, fundraising, and cross-border operations, Ramesh brings a founder-operator mindset to Secode. His current focus is on leveraging AI to solve enterprise-grade security and compliance challenges at scale, working closely with global tech and cybersecurity leaders.

https://www.linkedin.com/in/rameshbhandari1/

Mr. Manoj Neupane, Co-Founder

Mr. Manoj Neupane is a highly respected banking and finance leader with over 20 years of experience in Nepal's financial sector. He previously served as the **Chief Executive Officer of a Class A Commercial Bank**, where he led large-scale operations, regulatory compliance, risk governance, and balance-sheet management. As Chairman of the Board at Secode, he provides strategic oversight, institutional governance discipline, and deep insight into enterprise risk, regulatory expectations, and financial system security. His leadership anchors Secode's credibility with regulators, financial institutions, and institutional investors.

https://www.linkedin.com/in/manoj-neupane-b87542b1/

Mr. Divyendu Bhatt, Co-Founder & CTO

Mr. Divyendu Bhatt is a globally seasoned cybersecurity executive with over 25 years of experience securing large-scale enterprise and financial systems. His career includes senior leadership roles at **BCG** (Technology Security Advisor to the Group CTO), **JP Morgan Chase** (Director of Security), **PayTM Money (CISO)**, and Hewlett Packard Enterprise (Master-Level Consultant). He brings deep, hands-on expertise in application security, cloud security, enterprise risk management, and security product ecosystems. At Secode, he leads security architecture, threat modeling, and product trust, ensuring the platform is built with real-world attacker awareness and enterprise-grade rigor.

https://www.linkedin.com/in/dm-bhatt-0bb8a48/

Mr. Suresh Bhandari, Co-Founder

Mr. Suresh Bhandari brings over 25 years of experience across business consulting, ICT, and alternative energy sectors. He has advised and operated businesses across multiple industries, with strong expertise in financial management, accounting, and enterprise structuring. At Secode, he contributes strategic guidance on business scalability, financial discipline, and long-term value creation. His multi-sector operating perspective strengthens Secode's ability to execute sustainably while navigating complex commercial environments.

https://www.linkedin.com/in/sureshbhandari/

Mr. Tejash Raj Katuwal, Co-Founder & Engineer

Mr. Tejash Raj Katuwal is an AI engineer focused on building practical, production-ready intelligence systems. He has developed multiple AI-driven products and proof-of-concepts, with hands-on experience in applying machine learning models to real-world use cases. At Secode, he is responsible for embedding AI into security workflows, transforming complex security signals into actionable intelligence. His strength lies in delivering high-impact AI capabilities under constrained resources, enabling Secode to innovate rapidly while maintaining engineering efficiency.

https://www.linkedin.com/in/tejash-katuwal/

Mr. Ritesh Raj Pandit, Co-Founder & Engineer

Mr. Ritesh Raj Pandit leads product experience and interface design at Secode, bridging business logic with user-centered engineering. He specializes in translating complex security workflows into intuitive, functional, and visually refined interfaces. In addition to UI/UX execution, he plays a key role in defining business flows and product logic that guide engineering teams. His work ensures that Secode's advanced security capabilities remain accessible, usable, and adoption-ready for enterprise customers.

https://www.linkedin.com/in/riteshrajpandit/

Mr. Nibesh Suwal, Co-Founder & Engineer

Mr. Nibesh Suwal is a backend-focused architecture engineer with deep involvement in designing secure, scalable system infrastructures. He combines architectural planning with hands-on backend development, ensuring design decisions are grounded in execution reality. At Secode, he is responsible for core platform architecture, backend reliability, and secure resource allocation. His disciplined approach to system accuracy, optimization, and security underpins Secode's ability to operate as a trusted enterprise security platform.

https://www.linkedin.com/in/nibesh-suwal/

Mr. Abiral Bhandari, Co-Founder & Engineer

Mr. Abiral Bhandari brings a strong background in system analysis, architecture planning, and project execution, complemented by early experience in robotics. He specializes in translating business and security requirements into scalable technical architectures and delivery plans. At Secode, he leads engineering coordination and execution, ensuring optimal utilization of both technical and human resources to build enterprise-grade security products that meet performance, reliability, and scalability standards.

https://www.linkedin.com/in/abiralbhandari/

Augmented by advisors in cybersecurity and regulatory compliance.

12. Financial Projections (3-Year Summary)

Metric	Development Duration	Year 2	Year 3	Year 4
Revenue (ARR)	1 Year	$1.8M	$5.6M	$10.8M
Gross Margin		82%	84%	86%
Enterprise Clients		12	60	220
Developer Seats		6000	40000	150000

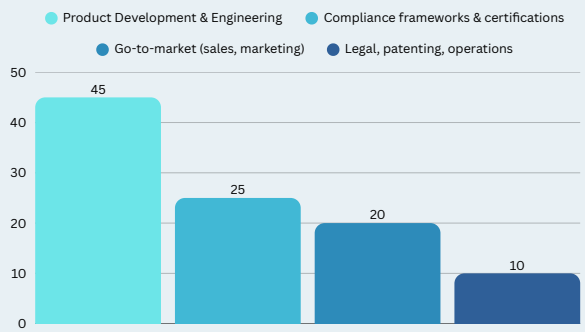
Projected break-even: Month 26
Revenue model validated by industry benchmarks.

13. Capital Requirements

Secode™ is opening a Pre-Seed Round of $1.1M
Valuation : USD 5.5M, Pre-Money

Use of Funds

- 45% → Product development & engineering
- 25% → Compliance frameworks & certifications
- 20% → Go-to-market (sales, marketing)
- 10% → Legal, patenting, operations



Milestones Post-Funding

- Patent and IP protection activities
- Full v1.0 release
- 10+ enterprise pilot deployments
- Launch of Compliance & Dataset products
- U.S., EU, and India regulatory alignment
- MLOps partner integrations

14. Exit Strategy

Potential exit paths include:

1. Acquisition by

- Cloud providers (AWS, Azure, GCP)
- MLOps platforms
- AI governance/enterprise security leaders
- Compliance tech platforms

2. Strategic Merger

With cybersecurity vendors expanding into AI safety.

3. Long-term IPO

If category leadership is maintained.

Given the regulatory tailwind, AI security is expected to consolidate significantly within 4–7 years.

15. Investment Proposition

Investors in **Secode™** gain exposure to:

- A new and rapidly expanding category (Pre-MLOps AI Safety)
- First-mover advantage with high defensibility
- Recurring revenue and enterprise-grade margins
- Regulatory alignment and compliance-driven demand
- Scalable architecture and strong GTM strategy
- Team with cross-domain expertise in AI and security

Secode™ is positioned to become the global standard for Trusted AI Development.

Conclusion

AI safety is no longer optional—it is a regulatory and operational requirement. Secode™ fills the most critical gap in the AI lifecycle by securing development itself. With increasing global mandates, strong technical validation, and zero competition in its category, Secode™ is uniquely positioned for rapid adoption and scale.

Investing now provides early ownership in a category-defining platform at the moment the market is forming.