Anthony Chisom

AI Security & Safety Engineer | AI Governance | Secure AI Systems Builder
anthonychisom872@yahoo.com · +234 8129675957 · Lagos, Nigeria (open to remote)
anthonychisom.dev · LinkedIn · GitHub

Engineer building the security and governance layer for AI systems. Has designed and built an MCP security shield that sits between an AI agent and its tools to stop malicious prompts, and is building a PII-swapping gateway that keeps personal data away from external AI models, mapped to GDPR and Nigeria's Data Protection Act 2023. Runs a live, AI-powered national platform on the Anthropic API with row-level security across 18 tables, bot protection, rate limits, spend caps and a human review queue for low-confidence AI output. Currently studying AI governance (safety and security). Brings 5+ years of risk control, scheduling and stakeholder coordination from construction and infrastructure delivery, and training in financial modelling that shapes how every system handles money, data and decisions.

Roles

AI Product Builder & Automation Specialist, Independent (Self-employed)

JAN 2026 - PRESENT
LAGOS / REMOTE

- Design, build, secure and deploy full-stack web apps and AI automations end to end, from requirements and data models to hosting, using AI coding agents (Claude Code).
- Ecclesia Nigeria: engineered an AI discovery engine (Anthropic API) that auto-publishes only events whose proof is quoted on the source page; everything else routes to a human review queue with confidence labels.
- Secured Ecclesia with row-level security across 18 database tables, bot protection (Cloudflare Turnstile), per-visitor rate limits, weekly backups and a daily cap on AI spend.
- The Fashion Store: set up owner and staff roles with role-based permissions so staff never see cash flow or profit.

Project Manager, Depcico

OCT 2023 - PRESENT
LAGOS

- Direct on-site operations for multiple construction and infrastructure projects at once, keeping schedules, budgets and quality standards on track.
- Track progress, costs and resources against approved plans from inception to handover, and report variances to management.
- Manage risk across projects and coordinate architects, engineers, contractors and crews to resolve problems and reduce delays and cost overruns.
- Introduced AI tools into project documentation and reporting, speeding up progress reports and analysis for management decisions.
- Manage personnel, materials and equipment to improve productivity and cost efficiency.

Field Engineer, Depcico

MAR 2021 - OCT 2023
LAGOS

- Supervised foundation and on-site construction activities to design specifications, quality standards and resource plans.
- Recorded and reported daily site progress, identifying variances and resolving technical issues before they caused delays or extra cost.

AI security work

MCP Shield Gateway

PROTOTYPE · 2026

A security gateway between an AI assistant and its MCP tools. It scans every tool for hidden orders, pins the approved ones, checks every call and keeps a tamper-evident log.

anthonychisom.dev/demos/mcp-tool-poisoning-shield.html ↗

PII Swapping Gateway

2026

Swaps personal data (BVN, NIN, phone, card and email) for random tokens before a prompt leaves for an outside AI model, then puts the real values back in the reply.

Products I have shipped

Ecclesia Nigeria

2026

One place to see every Christian gathering in Nigeria, day by day and state by state, kept current by an AI scanner and a human approver.

ecclesianigeria.com ↗

KudiTrail

2026

Answers one question for Nigerians: where did my money go? Drop a bank statement and see your month as a river.

kuditrail.vercel.app ↗

The Fashion Store

2026

A custom operations app that runs a clothing business from a phone: point of sale, live inventory, profit and loss, debtors and WhatsApp receipts.

trinaafashionstore.vercel.app ↗

Clipwise

2026

A free video editor and clipping tool that runs entirely in your browser. Your videos never leave your computer.

clipwise-xi.vercel.app ↗

Statement to Excel

2026

Paste a bank statement and get a clean, editable Excel file. Processed in your browser, never saved.

ghost-agent-psi.vercel.app ↗

AI Services Venture (Adullam Services)

2026

Web and app development, AI automation and video work for small businesses and creators.

adullam-olive.vercel.app ↗

Talks and workshops

AI Governance for Nigerian SMEs

WORKSHOP · 30 MINUTES · 12 SLIDES

The NDPA 2023 and the EU AI Act, turned into controls a small business can run on Monday: risk tiers, keeping personal data out of prompts, guarding AI agents, and a 90 day starter plan.

anthonychisom.dev/talks/ai-governance-nigerian-smes.html ↗

Skills

AI SECURITY & SAFETY

Agent and tool-call security · MCP security · Malicious prompt detection and blocking · Guardrails · Human-in-the-loop review · Confidence labelling · AI spend controls · Secure LLM integration (Anthropic API)

DATA PROTECTION & GOVERNANCE

PII detection, tokenisation and re-identification · Data minimisation · Privacy-by-design · GDPR · Nigeria Data Protection Act 2023 · Handling of Nigerian identifiers (BVN, NIN, card numbers) · Risk assessment · AI governance fundamentals

SECURE ENGINEERING

Row-level security · Access control and role-based permissions · Bot protection (Cloudflare Turnstile) · Rate limiting · Backups and recovery · Takedown and incident handling · Database design · Supabase (Postgres, Edge Functions, pg_cron)

AI & DEVELOPMENT

AI coding agents (Claude Code) · Prompt engineering · Workflow automation · Full-stack web apps · React · Node.js · JavaScript · SQLite · Vercel deployment

DELIVERY & FINANCE

Requirements gathering · Scoping · Risk mitigation · Quality control · Stakeholder management · Budgeting and cost control · Financial modelling and valuation

TOOLS

Claude · Claude Code · ChatGPT · Microsoft Excel · Word · PowerPoint · Microsoft Project

Certifications

AI Governance (Safety & Security)
IN PROGRESS

Project Management Foundations
LINKEDIN LEARNING · 2023

Financial Modelling & Valuation
TRAINING

ICAN (ATS), Finance & Accounting Professional Qualification
IN PREPARATION

Education

B.Eng in Mechanical Engineering
COVENANT UNIVERSITY, OGUN STATE, NIGERIA · 2022
SECOND CLASS UPPER

Research interests

I want to study how AI agents can be made safe to deploy in emerging markets: auditable, privacy safe and hard to trick, when they touch customer data and money in places like Nigeria. I plan to pursue graduate research at the intersection of AI security, governance and operations.