CAPABILITY STATEMENT

HoneyBee Tech & Innovations

A global, remote-first technology company that builds secure software, cloud and digital products — and trains the people who defend them.

Registered name	**HoneyBee Tech & Innovations**
Founded	**2023**
Delivery model	**Global · Remote-first**

Capability areas

Software Development

Custom platforms and internal systems built to a specification you own, with security designed in from the first commit.

Web & Mobile Development

Marketing sites, web applications and mobile apps that load fast, rank well and hold up under real-world use.

Cloud Solutions

Cloud architecture, migration and cost control — with identity, network boundaries and backups configured properly.

Cybersecurity

Assessment, hardening and incident readiness — findings ranked by real business impact, with the fixes done, not just listed.

DevSecOps

Pipelines that ship faster and catch security problems before they reach production — not after a customer finds them.

Full Stack

One team across the whole system — the architecture, the services behind it, and the payment rails it has to settle through.

UI/UX Design

Research, interface design and reusable design systems — accessible by construction, not by later remediation.

Digital Transformation

Sequenced modernisation of how the organisation works — prioritised by payback, delivered in stages that each stand alone.

IT Consulting

Independent technical advice — architecture review, vendor and build-versus-buy decisions, and due diligence.

How an engagement runs

Four stages, every time, whichever capability the work starts with. Nothing is built before the scope is agreed in writing, and nothing is finished until your team can run it without us.

01 **Conversation**
A call to understand the problem and say honestly whether we are the right people for it.

02 **Written scope**
Objectives, deliverables, security requirements, assumptions and price, in a document you approve before work starts.

03 **Delivery in increments**
Short cycles with something reviewable at the end of each, and security checks running in the pipeline throughout.

04 **Handover**
Documentation, runbooks, a walkthrough with your team, and full ownership of the code and accounts.

What you own at handover

Security is the default, not the upsell

Threat modelling, input validation, secret management and dependency scanning are included in every build engagement. You do not buy them separately, and we do not discover them at the end.

You own everything at handover

Repository, deployment pipeline, cloud accounts, documentation and runbooks. No proprietary layer you have to keep paying us to maintain, and no lock-in disguised as support.

Decisions in writing, before the build

Scope, architecture and the security model are agreed in a document you sign off. When something changes mid-project — and it will — there is a shared record of what changed and why.

Plain language, both directions

Technical reports for engineers, and the same findings written for the people funding the work. If a recommendation cannot be explained to a decision-maker, it is not finished.

Built to be maintained by your team

Conventional tooling, documented structure and a walkthrough at handover. We would rather you did not need us for routine changes.

We say when the answer is 'do nothing'

Some systems should be left alone and some projects should not start. Advice that only ever points towards more billable work is not advice.

How we evidence delivery

Every case study we publish has the same four parts, in this order. If a piece of work cannot be described this way, it does not go up.

Problem The situation before we were involved, described in the client's own terms — including what the status quo was costing them.

Approach	What we built or changed, and why we chose that route over the alternatives we considered.
Technology	The stack and infrastructure involved, so a technical reader can judge whether the work is comparable to theirs.
Outcome	The measurable result, with figures published only where the client has confirmed them in writing.

Nothing is published without written client approval — not a name, not a logo, not a figure. Any number that appears is one the client has confirmed in writing, and security work in particular is often contractually confidential. What we cannot publish we can usually discuss: comparable work walked through under an NDA, or an introduction to a reference.

Not yet confirmed

Stated plainly, because a procurement reader will ask and because the website does not claim otherwise:

- Country of registration — not yet published.
- Published case studies — none yet. The standard above is the commitment; the portfolio is empty by choice rather than by omission.

Contact

Email	honeybeedesignsx@gmail.com
Proposals	https://honeybeetechinnovation.com/request-proposal