NETWELL ENTERPRISE · PRIVATE AI INFRASTRUCTURE

Run your AI inside your office. Not on someone else's server.

For Malaysian SMEs handling confidential client data, generic cloud AI is no longer a defensible answer. Netwell installs private AI infrastructure on your premises, hardens it to a published security standard, trains your staff to use it safely, and maintains it month after month — so you can use AI without leaking your clients to a foreign cloud provider.

Three reasons cloud AI is now a problem

1. Your client data is leaving Malaysia. Every prompt typed into ChatGPT, Claude, or Gemini is processed on foreign servers, subject to foreign law and foreign subpoena. For lawyers, clinics, accountants, and manufacturers handling confidential information, this is an unaddressed PDPA exposure.

2. PDPA 2024 raised the stakes. Mandatory data breach notification, mandatory Data Protection Officer for qualifying organisations, materially higher penalties, and tightened cross-border transfer rules. If your AI use leaks data, the law no longer permits you to handle it quietly.

3. Your staff are already using AI — without rules. Junior employees paste contracts, patient notes, financial records, and internal documents into chatbots every day. There is no audit trail, no acceptable use policy, and no way to recall the information once it has left.

What Netwell does about it

We install a private AI server in your office, configured to the **Netwell Private AI Security Standard (NPAISS v1.0)**, integrated with your document workflows, and operated under a service agreement that keeps it patched, monitored, and reviewed. Your data does not leave your premises unless you explicitly authorise it — and when it does, it is logged, classified, and screened first.

Service tiers

Bronze — Foundation

For 5–15 user offices with low-to-moderate sensitivity workloads.

NPAISS v1.0 baseline build · ½-day staff awareness training · standard documentation pack · quarterly remote check-in · 30-day post-install support.

From RM 25,000 setup · from RM 800 / month

Silver — Professional

For 15–50 user practices in regulated sectors (legal, medical, accounting).

Bronze + 1-day administrator training + monthly health check + quarterly tabletop exercise + priority support + custom RAG corpora + DLP egress controls + signed NPAISS attestation pack.

From RM 60,000 setup · from RM 1,800 / month

Gold — Managed

For larger firms or high-sensitivity environments needing assured response.

Silver + 24/7 monitoring + SLA-backed response + annual full security review + on-call DPO advisory + customised model fine-tuning + dedicated account engineer.

From RM 120,000 setup · from RM 4,000 / month

What you receive at the end of installation

A working private AI deployment integrated with your business workflows. And a complete documentation pack you can produce to a regulator, an auditor, your insurance underwriter, or a tribunal:

- Privacy Notice covering AI processing
- Data Protection Impact Assessment (DPIA)
- Records of Processing Activities (RoPA)
- Information Security Policy — AI addendum
- Incident Response Plan — AI-specific
- Acceptable Use Policy — signed by every user
- Access Control Matrix
- Backup & Recovery Procedure
- Vendor & Dependency Inventory
- Training Records & Attendance Log

Plus one signed document that ties everything together: a **NPAISS v1.0 Attestation** naming the controls implemented, the evidence on file, and the next review date.

How we secure it — NPAISS v1.0

NPAISS v1.0 is our published security baseline. Every deployment is built and attested against 73 numbered controls across ten families:

INF — Infrastructure & Network	LOG — Audit, Logging & Monitoring
IDA — Identity, Access & Authentication	**EGR — Egress & Hybrid Cloud**
MOD — Model, Prompt & Guardrail	**OPS — Operational Security**
DAT — Data, RAG & Information Lifecycle	**COM — Compliance Documentation**
TRA — Training & Awareness	**IRP — Incident Response**

NPAISS is cross-mapped to the OWASP LLM Top 10, the NIST AI Risk Management Framework, and the seven principles of the PDPA — so your lawyer, your auditor, and your DPO can verify our claims against the frameworks they already use.

The standard is public. Ask us for a copy or download it from our site.

How we train your team

Module 1 — Awareness (½ day, all staff). What the AI is for, what must never go into it, how to recognise when something is wrong. Includes a live demonstration of a prompt-injection attack so your team sees the threat, not just hears about it.

Module 2 — Administration (1 day, IT and DPO). Operating the system, managing users, reviewing logs, recognising and responding to security events.

Module 3 — Annual tabletop (2–3 hours). Scenario-based incident drill for leadership, IT, and DPO. Outcomes feed plan revision.

Why this matters now

Two pressures are converging on every Malaysian professional firm:

- **Regulators are tightening** — PDPA 2024 amendments, Cyber Security Act 2024, NACSA bulletins, sectoral overlays from BNM, MOH, and others.
- **Operations are pulling AI in faster** — every month, more of your workflows touch a generative AI somewhere.

Doing nothing widens the gap between those pressures inside your organisation. Doing something hastily creates a different category of liability. Netwell is the local Malaysian option for doing it once, and doing it properly, with documentation you can defend.

WhatsApp: +6011-6118 5121 · **Email:** cninesix@gmail.com
Senai, Johor — visits by appointment.

Free 30-minute consultation. No commitment.