CyberTeam

GUIDE · V1.0 · MAY 2026

PROCUREMENT · LEGAL · RISK

AI vendor terms, de-fluffed.

What to look for, what to negotiate, and what to watch out for before you sign an AI services agreement with any major vendor.

AUDIENCE

Procurement, Legal, CIO/CISO

READ TIME

~15 minutes

PREPARED BY

CyberTeam

00

WHY THIS GUIDE EXISTS

AI contracts are where the risk actually lives.

As AI tools become embedded in enterprise operations, the contractual terms governing **data usage, model training, intellectual property and liability** carry significant legal and commercial weight. This guide summarises the key provisions every organisation should understand, negotiate, and monitor when entering into an AI services agreement with any major vendor.

> Procurement signs the contract. Engineering uses the tool. Compliance owns the blast radius. *This guide is for all three.*

What you'll find inside

01

THE CRITICAL CLAUSE

Data use and model training

This is the most critical area. The core question: **can the vendor use your data to train or improve their models?**

PREFERRED TERMS

- Vendor will **not** use your data (inputs, outputs, or usage data) to train models available to other customers or to public AI models.
- Third-party model suppliers are **also** contractually prohibited from training on your data.
- Any model customisations built using your data are **exclusively yours** and not shared with other customers.
- Data is used solely for the benefit of your organisation.
- Retention and deletion processes are clearly defined.

TRIGGER FURTHER REVIEW

- Broad rights to use "service data", "usage data", "telemetry" or "customer content" for **product improvement;** this can include your prompts and outputs.
- No explicit prohibition on training **third-party** models.
- Opt-**out** rather than opt-**in** approach to data use for training.
- Undefined data retention periods.

CYBERTEAM RECOMMENDATION

Insist on bilateral, contractually-bound training prohibitions.

Push for explicit, bilateral commitments: the vendor will not use your AI data (inputs, outputs, usage data) to train any model available to other parties, **and** will contractually bind their third-party model suppliers to the same obligation.

02

THE CRITICAL CLAUSE

Intellectual property & indemnification

Who owns the outputs? Who is liable if an output infringes a third party's IP rights? **The answers should be in writing, and the carve-outs should be narrow.**

● PREFERRED TERMS

- Vendor **indemnifies you** against third-party IP claims arising from AI outputs generated using the vendor's models.
- You retain ownership of your inputs and, where possible, your outputs.
- Indemnification carve-outs are **limited and specific** — not so broad they swallow the protection.
- Limitations or exclusions are clearly defined.

● TRIGGER FURTHER REVIEW

- Carve-outs so broad they effectively eliminate the indemnity — e.g. any output "related to" third-party content.
- **No indemnity for outputs at all** — some standard terms exclude this entirely.
- Unclear responsibility boundaries between vendor and customer.

Common carve-outs — standard and acceptable

Not every carve-out is a red flag. These are the ones a reasonable vendor will ask for, and a reasonable customer will accept.

CARVE-OUT	WHY IT'S REASONABLE
You breached the acceptable use policy	Vendor shouldn't cover wilful misuse.
Output came from your custom model or fine-tuning	Vendor didn't create that model.
You disabled safety filters	You circumvented the vendor's protections.
You modified the output	Vendor isn't responsible for your changes.
You solicited infringing outputs	Intentional misuse.

03

WHERE THE LIABILITY QUIETLY LANDS

Customer responsibilities

AI vendor agreements typically place significant responsibility on the customer. **Understanding these obligations protects you from liability.**

You are typically responsible for:

Lawfulness of all inputs.
You must have the right to submit the data you're providing.

Data protection compliance.
GDPR, the NZ Privacy Act, and equivalents — for any personal data in inputs.

Sensitivity assessment.
Deciding whether sensitive, regulated, or confidential information can be submitted to the platform.

Decisions made on outputs.
Vendor outputs are a tool, not a decision.

Human oversight.
Implementing checks for high-stakes decisions or where outputs may be biased or inaccurate.

Acceptable Use Policy compliance.
Knowing, and enforcing, the vendor's AUP across your organisation.

PRACTICAL IMPLICATION

Run three checks before any AI feature touches a business process.

(1) Do we have the right to use this data as an input?

(2) What human checks are in place before acting on outputs?

(3) Have we reviewed the vendor's Acceptable Use Policy for prohibited uses?

04

THEIR GOVERNANCE, YOUR PAPER TRAIL

Vendor AI governance & ethics commitments

Increasingly, AI vendor agreements include commitments about how the vendor develops and governs its AI systems. **These matter for your own compliance and risk posture.**

● PREFERRED TERMS

- Commitments to **responsible AI** practices — ethics policies, bias testing, ongoing monitoring.
- **Pre-deployment testing** of models for general behaviour and performance.
- Compliance with applicable AI regulations — EU AI Act and emerging NZ / AU frameworks.
- **Regular validation** and monitoring of model behaviour post-deployment.
- Governance over **third-party models** used within the service.

WHY THIS MATTERS

Regulators are asking, and your auditors will, too.

Regulators and auditors are increasingly asking organisations to demonstrate they have **assessed the AI tools they use** . Vendor commitments on governance are part of your due diligence paper trail.

05

THE CLAUSE THAT KEEPS RE-WRITING ITSELF

Vendor rights to update the terms

AI vendor agreements frequently give the vendor the right to update terms unilaterally. **This is an area where negotiation can make a significant difference.**

WHAT STANDARD TERMS LOOK LIKE

Vendor can update AI terms **at any time** with notice (often 30 days).

Continued use constitutes acceptance — meaning you have no practical choice but to accept.

WHAT NEGOTIATED PROTECTIONS LOOK LIKE

Updates that reduce vendor obligations or increase data use rights require **written agreement** from both parties.

Updates to key sections (data use, indemnification, definitions) can only be made by **signed written amendment**.

Continued use does **not** constitute acceptance of material updates.

On request, vendor will provide a **consolidated reissued version** incorporating only changes that are validly binding.

CYBERTEAM RECOMMENDATION

Make data use and indemnification amendment-proof.

Push to make the sections on **data use** and **indemnification** amendment-proof without written agreement. At minimum, ensure continued use cannot constitute acceptance of updates that increase the vendor's data rights or reduce their obligations to you.

06

BRING THIS TO THE NEXT VENDOR CALL

The negotiation checklist

Use this when reviewing any AI vendor agreement. For each provision, mark one of: **Confirmed, Negotiate, or Risk-accept.**

No training on customer data (inputs, outputs, usage)	☐ Confirmed	☐ Negotiate	☐ Risk-accept
Third-party model suppliers also prohibited from training	☐ Confirmed	☐ Negotiate	☐ Risk-accept
Model customisations exclusive to customer	☐ Confirmed	☐ Negotiate	☐ Risk-accept
IP indemnification covers outputs	☐ Confirmed	☐ Negotiate	☐ Risk-accept
Indemnification carve-outs are specific and limited	☐ Confirmed	☐ Negotiate	☐ Risk-accept
Material updates require written agreement	☐ Confirmed	☐ Negotiate	☐ Risk-accept
Continued use ≠ acceptance of updates	☐ Confirmed	☐ Negotiate	☐ Risk-accept
Vendor AI ethics & governance commitments documented	☐ Confirmed	☐ Negotiate	☐ Risk-accept
Acceptable Use Policy reviewed and acceptable	☐ Confirmed	☐ Negotiate	☐ Risk-accept
Preview / beta features covered by separate terms reviewed	☐ Confirmed	☐ Negotiate	☐ Risk-accept

07

DEFINITIONS DECIDE THE SCOPE

Key terms glossary

AI vendor agreements use specific terminology. **Understanding these definitions shapes how the protections apply.** Check each definition before signing, *small word changes here can rewrite the deal.*

AI Data

Inputs and outputs that are not customer data — typically prompts and generated responses.

Customer Data

Data you provide to the service, usually defined in the master agreement.

Covered AI Features

The specific AI features governed by the AI terms — check this list carefully.

Input

Anything you submit to an AI feature — prompts, queries, data extracts.

Output

What the AI returns — summaries, code, analysis, generated text.

Model Customisation

Fine-tuning a model on your own data to specialise its behaviour.

Pass-Through Terms

Terms from third-party model providers (e.g. OpenAI, Anthropic) that flow through to you.

Preview AI Features

Beta / preview features — typically outside the main AI terms and with fewer protections.

Usage Data

Metadata about how you use the service — often broadly defined; check whether it includes prompt content.

CyberTeam

READY WHEN YOU ARE

Need a second set of eyes on a real AI vendor contract?

We're a Wellington-based cybersecurity consultancy. We help NZ government agencies, healthcare organisations and regulated enterprises review, negotiate and govern AI vendor terms, alongside the broader risk picture.

Discover our approach →

GET IN TOUCH

tom@cyberteam.co.nz

Drop us a line, we'll come back to you within one business day.

VISIT

cyberteam.co.nz

Wellington · Auckland · Nationwide. NZ-owned, founder-led.