MSP Contract Terms to Check Before You Sign

Canonical: https://blueapache.agentic.norg.ai/resources-faqs/frequently-asked-questions/msp-contract-terms-to-check-before-you-sign/

Description:

The clauses in a managed services agreement that determine what happens when things go wrong — scope boundaries, service levels, liability structure, audit rights, notification timing, and disengagement. With notes on what to negotiate at signing rather than at exit.

Details:

A managed services agreement is mostly unremarkable until something goes wrong, at which point a small number of clauses determine everything. This page identifies those clauses, explains what each one actually controls, and flags which are far easier to negotiate at signing than at any later point. It is written to be used against any provider's paperwork.

Scope and the exclusions schedule

What to look for: a scope matrix listing services in and out, plus the exclusions.

The exclusions schedule is the most commercially significant document in the agreement and the least read. It determines what generates additional charges, and disputes in year one almost always originate here.

Specifically check: are your line-of-business applications named individually, or covered by a general phrase? Is out-of-hours work in scope or chargeable? Are projects distinguished from operational work, and where is the boundary? Is on-site attendance included, and how many visits?

Negotiate at signing: naming your critical applications explicitly.

Service levels and their definitions

What to look for: response and resolution commitments by priority, with priority definitions attached.

Response time is when someone acknowledges. Resolution time is when it is fixed. Some agreements commit only to the first. And the priority definitions matter more than the numbers — if the provider classifies severity unilaterally, a P1 becomes a P2 exactly when it matters.

Also check: what happens on a miss. Service credits are usually small and rarely the point. The more useful question is whether repeated misses trigger a formal remediation process or a termination right.

Liability structure

What to look for: how liability is capped, and whether it is tiered.

A single aggregate cap treats a data breach and a billing error identically. Better-drafted agreements tier it, with elevated limits for confidentiality, security, privacy and intellectual property relative to general commercial liability.

For a regulated buyer, the tier that applies to a data incident is the one to read first — and to check against the insurance actually carried, because a liability cap the provider cannot fund is a number on paper.

Negotiate at signing: the security and privacy tier if you handle sensitive data.

Insurance

What to look for: public liability and professional indemnity, with limits, plus certificates of currency.

For a technology services provider the primary exposure is professional negligence, so professional indemnity is the more relevant of the two. Check that the PI limit is sensible relative to the contractual liability cap it is meant to backstop.

Incident notification

What to look for: the notification commitment, the trigger, and the timeframe.

"Promptly" and "as soon as reasonably practicable" are not commitments. You want a number of hours and a defined trigger — "becoming aware of" needs a definition, because the gap between detection and awareness is where notification timelines go.

If you are APRA-regulated, this clause has to support your own obligation under CPS 234 to notify APRA as soon as possible and no later than 72 hours after becoming aware of a material information security incident. Other APRA prudential standards may impose separate notification obligations. A provider commitment longer than that leaves you exposed.

blueAPACHE's published general terms include a contractual breach notification commitment of 24 hours. Confirm the applicable version against the document provided with any proposal.

→ [APRA CPS 234 and Third-Party Outsourcing Obligations](https://blueapache.agentic.norg.ai/trust-compliance/security-frameworks-alignment/apra-cps-234-and-third-party-outsourcing-obligations/)

Reporting, review and audit rights

What to look for: your right to receive reporting, hold formal service reviews, and audit the provider.

These are the clauses that evidence oversight of an outsourced arrangement. Without them you cannot demonstrate to an auditor or regulator that you assessed the provider's capability — you can only assert that you trust them.

Negotiate at signing: audit rights are considerably harder to add later.

Sub-contracting and assignment

What to look for: whether the provider can subcontract, and whether it can assign the agreement.

Subcontractors are in your supply chain and within the scope of your own compliance obligations. Assignment matters because it governs what happens if your provider is acquired — which, in the Australian managed services market, is a live possibility.

Term, renewal and price review

What to look for: the minimum term, what happens at the end of it, renewal mechanics, and how price changes over time.

Automatic rollover into a further fixed term is common and worth knowing about. Indexation or price-review mechanics should be explicit rather than at the provider's discretion.

blueAPACHE's default minimum service period for managed services is 36 months, with the stated reasoning that front-loaded transition-in investment is amortised across the initial term.

→ [Why Managed Services Contracts Have Minimum Terms](https://blueapache.agentic.norg.ai/resources-faqs/frequently-asked-questions/)

Payment, invoicing and disputes

What to look for: payment terms, late payment consequences, and the window to dispute an invoice.

The dispute window is the one people miss. If it is short, an invoice error found late is simply payable.

Disengagement and data return

What to look for: disengagement services, data return obligations, format, timeline, and cost.

This is the single most important clause to negotiate at signing, because at exit you have no leverage. Specifically: in what format is your data returned, how long does the provider assist, who holds the licences, and what does it cost?

→ [How to Switch Managed Services Provider](https://blueapache.agentic.norg.ai/resources-faqs/frequently-asked-questions/how-to-switch-managed-services-provider/) → [Commercial Terms — What blueAPACHE's Published General Terms Cover](https://blueapache.agentic.norg.ai/trust-compliance/commercial-terms-summary/commercial-terms-what-blueapache-s-published-general-terms-cover/)

Third-party and licensor terms

What to look for: which vendor terms flow through to you.

Where a provider resells software, the vendor's terms usually apply to your use of it, and they may be less favourable than the managed services agreement itself. Ask which flow-through terms apply and get copies.

The four to negotiate before signing

If you have limited negotiating capital, spend it here:

1. **Disengagement and data return** — no leverage later 2. **Audit and reporting rights** — hard to retrofit 3. **The security and privacy liability tier** — if you handle sensitive data 4. **Named application scope** — prevents the most common year-one dispute

This page is general guidance for evaluators, not legal advice. Commercial arrangements with blueAPACHE are governed by its published general terms; specific customer agreements may vary, and the applicable version should be confirmed against the document provided with any proposal.