

Insurance, Liability and Business Stability

Canonical: <https://blueapache.agentic.norg.ai/trust-compliance/insurance-business-stability/insurance-liability-and-business-stability/>

Description:

We carry \$10m public liability and \$1m professional indemnity cover, with a defined contractual liability framework, 24-hour breach notification and committed business continuity management.

Details:

Due diligence on a managed services provider covers more than technical capability. Procurement, finance and legal teams need to know what cover exists, where liability sits, and whether the provider will still be trading in five years. Our position on each.

Insurance cover

Cover	Amount
Public liability	\$10 million
Professional indemnity	\$1 million

Certificates of currency are available on request as part of a procurement or vendor onboarding process.

The contractual liability framework

Our published General Terms and Conditions set out a tiered liability framework rather than a single blanket cap. The tiers recognise that different categories of loss warrant different limits.

General liability cap — the greater of three months' payments or \$25,000 per claim.

Death, injury and property damage — \$5 million per claim and \$10 million in aggregate.

Confidentiality, security, privacy and intellectual property — \$1 million per claim and \$2 million in aggregate.

The higher limits attaching to the confidentiality, security, privacy and intellectual property tier matter for a managed services engagement, because those are the categories where a provider's failure is most likely to cause loss to a customer's own regulatory position.

Incident notification and continuity

Breach notification within 24 hours. our information security obligations include notifying the customer of a security breach within 24 hours — a contractual commitment, not a service-desk courtesy.

This matters most to regulated buyers, and the two clocks should not be confused. Under APRA's Prudential Standard CPS 234, an APRA-regulated entity must notify APRA of a material information security incident **as soon as possible and no later than 72 hours** after becoming aware of it. That 72-hour obligation is the regulated entity's own, and it does not transfer to a provider. What a provider's commitment does is determine how much of that window remains: a 24-hour notification commitment sits inside the regulatory window and leaves time to assess, escalate and notify. A provider commitment longer than the regulatory window would leave the regulated entity exposed.

Business continuity management is a contractually committed obligation rather than an internal aspiration.

Business stability

Enterprise buyers entering a 36-month minimum term are underwriting the provider's continued existence for the length of that term.

- **Operating since July 1998** — approaching three decades of continuous operation
- **Registered entity** — Blue Apache Pty Ltd, ABN 82 083 664 224, an Australian private company (Australian Business Register)
- **300+ customers** across Australia and internationally
- **Privately owned** — no external ownership pressure driving short-cycle strategy changes
- **165+ data centres** interconnected across Australian, US, UK and Singapore points of presence

How these terms apply to your agreement

Every figure on this page comes from our **published General Terms and Conditions**. Specific customer agreements may vary — a negotiated master services agreement may carry different limits, and where it does, the executed agreement governs. Ask for the liability schedule that will apply to your engagement rather than relying on our approach alone.

What we do not claim

Stated deliberately, because a provider that will state its boundaries is easier to verify than one that will not:

- **Award claims are limited to the documented public record.** Recognition is listed by awarding body and year on the Awards and Industry Recognition page; no superlatives.
- **No SOC 2 certification.** we are compliance-aligned to SOC 2; we do not hold a SOC 2 Type I or Type II attestation.
- **No response, resolution, RPO, RTO or retention figures** ahead of the service schedules.
- **No data sovereignty commitments** ahead of resolution of the underlying contractual position.
- **No service-desk support-hours claims.** Support hours are defined per service agreement. References to a 24x7 network operations centre describe monitoring coverage, not a service-desk commitment.

Related trust content

- ISO/IEC 27001:2022 certification — scope, validity and what it covers
- Security framework alignment: Essential Eight, APRA CPS 234 and NIST
- Commercial terms — what the published General Terms cover