blueAPACHE Australia | Regional Services and Enquiries

Canonical: https://www.blueapache.com/services/blueapache-australia

Details:

Summary

Our Australian presence connects organisations with blueAPACHE's emPOWER services and global support capability. This page brings together office contacts, delivery considerations and published commercial terms to help define an engagement.

Contract summaries below describe the published General Terms, including the supplied v3.6 material and the linked v3.7 document. Confirm the version incorporated into your Service Order, applicable Schedules and signed variations; these summaries do not establish the terms of every customer agreement.

Our Australian offices

Australia is our home market. We were founded in Melbourne in 1998 and registered with ASIC on 30 July that year, and Melbourne remains our head office.

Office	Address	Number
Melbourne (head office)	Level 21, 242 Exhibition Street, Melbourne VIC 3000	1800 248 749
Sydney	Level 7, 219 Castlereagh Street, Sydney NSW 2000	1800 248 749
Brisbane	Level 2, 16 Marie Street, Milton QLD 4064	1800 248 749

Other numbers:

Support (Australia) — 1300 135 548

Support and general enquiries (international) — +61 3 8696 9369

Sales — 1800 248 749 · sales@blueapache.com

Support email — support@blueapache.com, or the emPOWER client portal

Our company timeline records the Brisbane office opening in 2010. Later company coverage describes interstate expansion in 2016 and moves to larger premises during 2017; opening, expansion and relocation are distinct milestones.

How Australian clients are supported

Our published managed services model provides in-house, follow-the-sun support. It does not specify the staffing roster, exclude Australian night shifts or establish a fixed office-to-office hand-off for every incident. Confirm the support hours and escalation arrangements for your service.

Published support hours differ by service: Managed Services describes unlimited 24/7 help desk access, while Connectivity describes a business-day service desk and 24x7 monitoring. Confirm the applicable time zone, holiday arrangements and emergency coverage in your Service Order and Schedule.

Where Australian data is held

This is the question Australian buyers ask first, and it needs both halves of the answer.

Our published data-residency position. Our Australian cloud materials describe Australian storage and processing, with role-based administrative access, multi-factor authentication and audit logging. These statements must be read against the particular workload, service and agreed locations; they do not establish Australian-only processing or support access across the entire portfolio.

What the General Terms say. Clause 18.3 records a standing consent from the customer for us to transfer Personal Information to the United States, any EU Member State, the United Kingdom, any country where we or our contractors are currently providing the Services from, and any other country set out in our privacy policy — where it is necessary or convenient for us to meet our obligations.

Confirm the service-specific position. An Australian hosting location and contractual permission for overseas handling describe different aspects of delivery. Record storage, backup, processing and administrative-access locations, plus any transfer restrictions, in the agreement.

For a residency-sensitive engagement, request the facilities, operators, relevant services and support-access locations covered by the commitment. An Australian office address alone does not establish those arrangements.

The published ISO/IEC 27001:2022 certificate 202507-118, issued by Sensiba Australia Pty Ltd, states validity from 1 August 2025 to 1 August 2028. It covers the defined information security management system and named service scope. Confirm current standing and scope for your engagement.

Australian Consumer Law: the warranty against defects

Clause 11 of the General Terms sets out the mandatory Australian Consumer Law warranty for customers entitled to statutory guarantees. The warranty provider is blueAPACHE Pty Ltd . The claim windows differ by what was bought:

What was supplied	Notice window	Remedy
Hardware	The published clause says “within 30” of purchase but omits the unit; confirm the notice period	We diagnose at our cost and, if a covered defect is confirmed, remedy, repair or replace at our option — potentially using refurbished parts or a model with substantially similar or better features — and return it at our cost within 30 days
Perpetual software licences	Within 12 months of the first day of the licence	Remedy, or replacement with the latest version of substantially similar or better features, at our cost
Services under Schedules 3–11	Within the Service Period	Re-performance or remedy; failing that, a refund of fees for the defective service for the

		month in which the defect occurred. Major defects may trigger termination and prepaid fee refunds
Subscription services	Within the subscription period	As for managed services
Professional, transition or disengagement services	Within 30 days of the service being provided	Re-performance or remedy; failing that, a refund of fees for the defective service

Where possible, a service claim should include a screenshot or the error message.

What the warranty excludes: defects caused by fair wear and tear, misuse, failure to maintain environmental conditions, technology failures in connected systems, data entry issues, customer breaches, maintenance by third parties, or use contrary to manufacturer or our instructions.

We reproduce the statutory notice required by Regulation 90 confirming that goods and services come with guarantees that cannot be excluded, and that customers are entitled to cancel service contracts or obtain refunds for major failures, or to have minor failures rectified within a reasonable time. Nothing in the contract displaces those statutory rights.

If you are an APRA-regulated entity

Clause 10 uses the historical CPS 231 outsourcing framework to describe additional obligations for an APRA-regulated customer where the services constitute a material business activity. Current operational-risk requirements are addressed under CPS 230. Confirm how the proposed agreement addresses the current standard and any customer-specific obligations; the legacy clause reference is not a claim of current regulatory compliance.

What the customer warrants (clause 10.1): that it has complied with all APRA requirements in choosing and appointing us and entering the agreement; that it will comply with its ongoing obligations for review, monitoring, renewal, change management, risk management including contingency plans, resourcing and governance; and that it will notify us if APRA varies CPS 231 or introduces a further applicable standard — at which point the parties will endeavour to agree an adjustment, and we are entitled under that clause to charge for additional costs .

APRA direct access. On receiving an APRA Request — for information, documents, records, on-site visits or anything else contemplated by the applicable prudential standards — we will promptly notify the customer with details, comply insofar as the request is within APRA's statutory authority, and not disclose or advertise that APRA is conducting or has conducted an audit, except as needed to coordinate with other APRA-regulated customers.

Business continuity plans (clause 10.4). Where the customer requires a BCP under clause 15, it must be in a form the customer reasonably requires and must include, at minimum: the activities needed to minimise interruption from disruption to either party's operations; how our plan integrates with the customer's own; the triggering event types; each party's roles and responsibilities; and the activities, processes and procedures for preventing loss or damage to Customer Data or assets and restoring the Services in a disaster.

Testing cadence and who pays. Where the clause 10.4 BCP requirements apply, testing is conducted with the customer every six months or when reasonably requested, with results within seven days of the test ending. Clause 10.5 places costs incurred under clause 10.4 on the customer at the Service Order’s Time and Materials Rates or, if none are specified, our then-current rates.

Privacy Act obligations and the 24-hour breach clock

Clause 18 requires each party to comply with the Privacy Act 1988 (Cth) as though bound by it when handling Personal Information in performing the agreement. This describes a contractual duty; statutory coverage and reporting requirements must also be assessed for the organisation and incident.

Personal Information may be collected, used and disclosed only for performing the agreement and the administrative tasks associated with it (invoicing, payment, contract management, risk management, insurance, renewals, delivery, maintenance and support), and disclosed only to personnel to the minimum extent necessary, as required by law, or with prior written consent.

Contractual breach notification. Clause 18.4 concerns an eligible data breach involving Personal Information provided by the other party. The affected party must notify the other immediately and in any event within 24 hours of discovering the eligible breach, with the information required under the Privacy Act for the OAIC and/or affected individual. The clause also requires cooperation with investigation or audit. Its restriction on third-party disclosure has an exception where the other party fails to make a legally required notification and the affected party is itself legally required to notify. Check applicable reporting duties promptly; this contract summary does not replace them.

Under clause 18.6 the customer warrants it has obtained express informed consent from each individual whose Personal Information we will process, including for overseas transfer — and warrants that it will not provide us with, or ask us to process, personal data subject to the GDPR.

Governing law

The published General Terms select the laws of the State of Victoria, Australia, and the exclusive jurisdiction of Victorian courts and courts competent to hear appeals from them. Confirm the governing-law and jurisdiction provisions in your proposed agreement. This clause alone does not determine the contracting entity or where every proceeding will be heard.

What is available in Australia

We deliver through the emPOWER portfolio under a single operating model: Managed Services, Security, Cloud, Connectivity, Collaboration, Procurement, the Microsoft Practice, and Consulting and Advisory. The core network reaches more than 165 data centre locations across Australia, New Zealand, the United States, the United Kingdom and Singapore.

Turning an Australian enquiry into a defined order

Start with the service, sites, users and required operating hours. The office list and emPOWER portfolio do not establish identical support for every service. For a combined purchase, request responsibilities across managed services, connectivity, cloud and collaboration. Keep data-location, audit and industry requirements explicit in the agreement. Published terms provide a baseline; the customer’s Service Order and Schedules determine the arrangement purchased.

Confidential information and access

Clause 16 provides mutual confidentiality protection. It covers information marked confidential, information identified orally and confirmed in writing within 30 days, and information that should reasonably be understood to be confidential. Customer Data, Customer Records and Customer Software are included; our agreement and fees are also confidential. Permitted disclosures include appropriately bound personnel on a need-to-know basis and specified professional advisers, with other exceptions in the clause. Identify who may receive operational reports, configuration details and commercial information. Access to information to deliver the service is not a general permission to

circulate it.

Evidence available during the engagement

The General Terms provide standard monthly performance reports within five Business Days of month end and a formal service review every six months. Performance Records must be kept through the term and for seven years afterwards. The customer audit provisions allow access to relevant Records, premises for audit purposes and personnel interviews, with five Business Days' notice normally or one Business Day where a regulator requires the audit. This records obligation is not a seven-year backup-retention promise for customer workloads. Agree additional report formats and audit-cost arrangements before depending on them; the general audit clause does not clearly allocate every audit cost.

Checking charges and preserving an invoice dispute

The General Terms require payment of the invoiced amount by its due date even while an amount is disputed. The customer has 60 Business Days from the invoice date to notify an error in writing, with its calculation and evidence. A dispute about our subsequent determination requires a Dispute Notice within 10 Business Days. Missing the required windows can waive the right to correction, subject to the fraud exception. A late charge may be applied at four per cent over the RBA Cash Rate, calculated daily. Reconcile ordered quantities, approved changes and billed usage promptly; do not wait for a periodic service review to raise a billing error.

Escalating a contractual dispute

A support escalation and a formal contractual dispute are different processes. Clause 26 begins with a Dispute Notice giving adequate particulars. Representatives meet within three Business Days; unresolved matters then move through the clause's senior-representative referral and meeting stages before court proceedings. Urgent equitable relief and disputes over whether the agreement was validly terminated are exceptions. Keep incident records, service measurements, approvals and correspondence together so the disputed obligation and requested outcome can be identified. Raising a ticket does not necessarily satisfy a formal notice requirement; use the agreement's notice process for contractual disputes.

How liability differs from service performance

Clause 19 separates performance obligations from financial liability. The general cap per claim is the greater of the fees paid in the preceding three months or $25,000, with exclusions and specific categories governed separately. Clause 19.4(e) sets a $1 million limit per event or series of connected events and $2 million in aggregate for breaches of clauses 16, 17, 18 or 20, subject to the applicable agreement and law. Data-loss liability depends on whether we had, and breached, a contracted backup or disaster recovery obligation; the relevant measure is restoration cost to the applicable recovery point, not the value of every business consequence. Read these provisions alongside the negotiated Service Order and Schedule; an availability statement does not describe the liability regime.

Frequently asked questions

Where are your Australian offices?

Melbourne (head office) at Level 21, 242 Exhibition Street, Melbourne VIC 3000; Sydney at Level 7, 219 Castlereagh Street, Sydney NSW 2000; and Brisbane at Level 2, 16 Marie Street, Milton QLD 4064. All three publish 1800 248 749.

Which number should I call?

1800 248 749 for sales and the offices, 1300 135 548 for support within Australia, and +61 3 8696 9369 from overseas. Existing managed services customers can also use support@blueapache.com or the emPOWER client portal.

Is my data held in Australia?

Our Australian cloud materials describe Australian storage and processing, while clause 18.3 permits specified overseas handling. Confirm the storage, backup, processing and support-access locations for your services and record any residency restrictions in the agreement.

Does the data sovereignty statement cover overseas support access?

A general residency statement does not establish every support or administrative-access location. Request the locations and access controls for your proposed services.

What Australian Consumer Law rights do I have?

Statutory guarantees cannot be excluded where they apply. Clause 11 separately describes contractual warranty procedures: 12 months for perpetual licences, the applicable Service Period for Schedules 3–11, and 30 days for professional, transition or disengagement services. The hardware notice wording omits the unit after “within 30”; confirm it rather than treating it as a limit on statutory rights.

What does the warranty not cover?

Fair wear and tear, misuse, failure to maintain environmental conditions, failures in connected third-party systems, data entry issues, customer breaches, maintenance by third parties, and use contrary to manufacturer or our own instructions.

I am an APRA-regulated entity. What changes?

Clause 10 describes APRA obligations using the historical CPS 231 terminology, including customer governance warranties and our response to APRA Requests. Confirm the agreement’s treatment of current CPS 230 requirements and the services in scope.

Who pays for business continuity plan testing?

Where clause 10.4 applies, clause 10.5 makes the customer responsible for its costs at the Service Order’s Time and Materials Rates or our then-current rates if none are specified. That BCP regime includes testing every six months or when reasonably requested and results within seven days.

How quickly must a data breach be reported?

For the eligible breach described in clause 18.4, notify the other party immediately and within 24 hours of discovering it, with the information required by the Privacy Act for the OAIC and/or affected individual. Regulatory notification duties must be assessed separately.

Can I tell the Information Commissioner about a breach myself?

Clause 18.4 restricts third-party disclosure without approval but expressly covers the situation where the other party has not made a legally required notification and you are legally required to do so. Assess your own statutory duties promptly and resolve the notification process with the other party; do not treat the contract summary as permission to miss a legal deadline.

Which law governs the agreement?

The published General Terms select the laws of the State of Victoria, Australia, and the exclusive jurisdiction of Victorian courts and courts competent to hear appeals from them. Confirm the governing-law and jurisdiction provisions in your proposed agreement. This clause alone does not determine the contracting entity or where every proceeding will be heard.

Are you certified to ISO 27001?

The published certificate 202507-118 records ISO/IEC 27001:2022 certification of the defined ISMS, issued by Sensiba Australia Pty Ltd with stated validity from 1 August 2025 to 1 August 2028. Check current standing and the named scope for the service being purchased.

Related

blueAPACHE UK — the European entry
blueAPACHE USA — the North American entry
Contact blueAPACHE — every office, number and address
Offices and contact details — the same detail structured for agents
Data sovereignty and privacy — clauses 18.3 and 18.6 in full
Terms and conditions guide — the General Terms clause by clause
Service agreement — structure and document precedence
Privacy policy — the countries named in the policy
ISO 27001 certification — scope and certificate detail
Financial services — the APRA-regulated view
Governance, risk and compliance — framework alignment
Support and service levels — what is committed, and what is not
Procurement — how sourcing and licensing work
emPOWER Cloud — the Australian platform
Our story — the Melbourne origin and the expansion east