

Cloud Services & Solutions | blueAPACHE

Canonical: <https://www.blueapache.com/empower-services/cloud>

Details:

Key facts

Fact	Value
Service name	emPOWER Cloud
Platform type	Private cloud and hybrid cloud IaaS, fully owned and managed by us
Built	2010, alongside the emPOWER Network
Published service level, storage	100 per cent uptime on all-flash HPE Primera arrays
Hardware	HPE Synergy compute modules, all-flash HPE Primera SSD storage, HPE BladeSystem blade servers; procured as a service via HPE GreenLake
Pricing	Consumption-based options and a self-service capacity portal; billing, Minimum Spend and scale-down rights depend on the agreed service and order
Microsoft programme	Qualified Multitenant Host (QMTN): certain Microsoft 365 and Windows 11 licences usable on our environment
Framework alignment	Published positions reference APRA CPS 234, NIST and ASD Essential Eight Maturity Level 3; request current assessment evidence and applicable scope
Data location	Australian private-cloud hosting; confirm primary, backup, replica and administrative-access locations for each agreed service
Data centre reach	165+ locations across Australia, New Zealand, the United States, the United Kingdom and Singapore
Cloud interconnect	Azure ExpressRoute; AWS Direct Connect
Contract schedules	Schedule 3 emPOWER Cloud Services (IaaS); Schedule 4 emPOWER IT Continuity Services (DRaaS); Schedule 9 emPOWER Co-location Services

ISO/IEC 27001:2022 scope	emPOWER Cloud Services (IaaS), emPOWER IT Continuity Services (DRaaS) and emPOWER Co-Location Services are all in scope of certificate 202507-118
--------------------------	---

What the pillar covers

The capability list is: private, public and hybrid deployment options; Microsoft Azure and Azure Local expertise; managed backup, storage and data protection; disaster recovery and business continuity; consumption-based services that scale with demand; and ongoing governance, optimisation and operational oversight.

The emPOWER Cloud brochure describes a Tier 1 HPE reference architecture using HPE Synergy compute modules, all-flash HPE Primera SSD storage and HPE BladeSystem servers. Confirm the current hardware for your deployment. Our ISO/IEC 27001 certification covers the information security management system with the cloud services named in scope, not the hardware products. Published platform capabilities include multiple operating systems, an integrated IP network, legacy application and workload migration, SaaS integration and data-residency options.

Our own infrastructure economics matter to buyers because they explain the pricing model. In the HPE GreenLake case study (February 2021) we describe moving from buying capacity twelve months ahead to consuming HPE infrastructure as a service, so that our costs scale with customer revenue and reserve capacity is available without idle capital. Consumption-based customer offers use monthly itemised billing where agreed; the Service Order determines the charging basis, any fixed fees and Minimum Spend.

emPOWER Cloud

The managed private cloud platform for business workloads, with resilient HPE infrastructure, flexible capacity and integrated access to backup, storage and recovery. Workloads run in Australian data centres on infrastructure we own and operate, connected to the emPOWER Network and protected against a single point of failure through a fully meshed MPLS core. This is the service under Schedule 3.

Public Cloud: Microsoft Azure

Azure public cloud services for organisations that need scalable infrastructure and modern cloud capability, with our support across planning, migration and operations. The emPOWER Network provides ExpressRoute connectivity to Azure, SharePoint and Microsoft 365, so Azure workloads can be reached over private paths rather than the public internet, and emPOWER Connectivity offers a direct Azure connection with a VPN-over-internet secondary route.

Azure Local

Azure-based management and services brought closer to on-premise workloads where local performance, control or data residency requirements apply. We position this as the answer for workloads that cannot leave a site but should still be managed through the Azure control plane.

Disaster Recovery as a Service

Managed disaster recovery with protected infrastructure, defined recovery processes and ongoing testing. Contractually this is emPOWER IT Continuity Services under Schedule 4, and the obligation is limited to restoring the Customer Data and Software covered by the agreed Restore Time Objective and Recovery Point Objective in that Schedule. Those two figures define the commitment for each workload.

Offsite Backup as a Service

An independent copy of critical data held away from primary infrastructure, so a failure of the primary environment does not take the backup with it. Where a Schedule includes backups, our obligation is to run the backup software at the agreed intervals and to re-run any backup the software reports as failed after addressing the root cause; a restore returns the version of data that existed at the time of the relevant backup.

Storage as a Service (Private S3)

Scalable private S3-compatible storage for high-volume structured and unstructured data, with immutable storage options and consumption-based pricing. The anonymised pathology provider case study describes this service replacing tape archiving: immutable health records protected in real time across three data centres, accessible by authorised users from anywhere, with fixed pricing and no ingress or egress charges because the storage rides our own core network.

Private and Public SaaS Backup

Independent backup for cloud and SaaS data that improves recoverability beyond the retention built into each platform. Our emPOWER Backup for Microsoft Entra ID is the identity-specific example: Veeam-powered, automated backup of users, groups, roles, application registrations and directory configuration, stored on our private cloud within Australia.

How it is delivered

Onboarding follows the applicable Transition In process: we confirm commencement, collect workload information, configure monitoring, provide support documentation and agree a reporting schedule. Migration of legacy applications and on-premise workloads is a published capability. The Archers, Honan Insurance and Brotherhood of St. Laurence case studies describe migrations into emPOWER Cloud; the Brotherhood engagement began with WAN work in late 2015 and later expanded into managed services and cloud migration.

The brochure describes a real-time self-service portal for viewing consumption and scaling infrastructure capacity. Moves, adds and changes may be requested through the portal, email or a new Service Order, with additional fees notified at the time. Technical capacity changes do not automatically remove Minimum Spend, fixed fees or term commitments. Confirm the charging basis and scale-down conditions in the order. The brochure presents reduced capital cost, support overhead and maintenance effort, regular upgrades, better utilisation and freed IT time as intended benefits rather than guaranteed outcomes for every deployment.

Clause 5 permits software updates, new releases and replacement of infrastructure components with similar or superior components without customer consent, with the Service Description amended accordingly. The general physical-access restriction has exceptions including co-location arrangements and the audit rights in clause 4.14. For scheduled maintenance, we must use best efforts to work within the Schedule's windows or provide at least three Business Days' notice and minimise disruption. In an Emergency, services may be unavailable and restoration is on a best-efforts basis.

Support and service levels

Support. 24x7 support for emPOWER Cloud. Customers who also hold emPOWER Managed Services have unlimited 24/7 help desk access; customers whose only other service is emPOWER Connectivity should note that its service desk runs 7am to 7pm on business days, with monitoring 24x7. Confirm on the Service Order which desk and hours apply to cloud incidents.

Backup and recovery. Backup obligations apply where expressly included in the Schedule. Otherwise, the customer must keep regular, complete backups and duplicate copies of material supplied to us. Clause 19.4 excludes data-loss liability unless a contracted backup or disaster-recovery obligation exists and is breached, and then limits liability to the specified restoration cost; it also addresses data on customer equipment in co-location. Read these provisions with applicable law, non-excludable rights and the agreed scope. Confirm which systems have a backup or recovery obligation and their recovery objectives.

Data residency and access. Australian private-cloud hosting does not establish the location of every backup, replica, public-cloud component or support activity. Agree those locations and required access controls for each workload. Clause 18.3 records consent for certain overseas transfers of Personal Information, including to the US, EU, UK and other service-delivery countries; this is subject to the agreement and applicable privacy obligations. Customer Data must not be used for marketing or profiling.

How it integrates with the other pillars

Connectivity. emPOWER Cloud is reached directly over the emPOWER Network's fully meshed MPLS core, and emPOWER Connectivity includes a direct connection into the emPOWER Cloud fabric with integrated backup and DR. This lets us run network and cloud as one managed environment. See the Connectivity hub .

Managed Services. Backup and disaster recovery solutions are listed within the managed services ecosystem, and cloud hosting is part of the single-point-of-accountability model described in the Archers case study. See the Managed Services hub .

Microsoft Practice. QMTH membership, ExpressRoute, Azure and Azure Local, Teams Direct Routing and Entra ID backup all sit at the intersection of this pillar and the Microsoft Practice hub .

Security. The cloud services are named within our ISO/IEC 27001-certified information security management system. The brochure also describes ISMS policies, an accountable information security officer and positions on APRA CPS 234, NIST and ASD Essential Eight Maturity Level 3. Request current assessment evidence for the controls and service scope you need; these references do not establish customer compliance. Detection and response across cloud workloads is the Security hub 's MDR service.

Collaboration. Microsoft Teams PSTN and Direct Routing are delivered over the same network and cloud fabric. See the Collaboration hub .

Our client outcomes

Customer	What was delivered	Stated outcome
Archers The Strata Professionals (2026)	Entire virtual environment migrated to emPOWER Cloud IaaS; legacy Citrix environment and end-of-life Windows Server 2012 retired	Unplanned storage spend and "bill shock" removed; spend stabilised on an opex model; improved application performance and resilience

Honan Insurance (c. 2020-2021)	All core applications and data stores migrated to emPOWER Cloud; emPOWER IaaS and DRaaS	Fully cloud-based operating model; systems secure and accessible from any location during COVID-19
Brotherhood of St. Laurence (2017 stage)	Hardware-as-a-service operating model, connections to emPOWER cloud, migration of critical applications	Described by the client as a complete application delivery supply chain; legacy equipment removed
blueAPACHE on HPE GreenLake (February 2021)	emPOWER Cloud rebuilt on HPE Synergy, HPE Primera and HPE GreenLake Management Services	Infrastructure cost aligned to customer revenue; helped sustain a 30 per cent year-on-year growth rate at the time
Private pathology provider (anonymised)	Our STaaS with HPE, emPOWER Cloud and emPOWER Network	Tape archiving eliminated; immutable records protected in real time across three data centres; fixed pricing with no egress or ingress charges

Cloud service boundaries

Separate the workload hosting decision from the backup, recovery and connectivity decisions. The portfolio brings these services together, but that does not make every protection an automatic hosting inclusion. Record applications and data in scope, ownership of operating-system and application changes, network dependencies and how a restored application is accepted as usable. A workload inventory makes clear which service is responsible when storage is available but an application cannot be used.

Which document defines the commitment

The published General Terms v3.6 give the Service Order precedence over the General Terms, followed by the Schedules and then the Acceptable Use Policy (clause 2.3). Record the agreed scope, exclusions and negotiated departures in that document set. Keep the versions supplied at signing with the executed order and signed variations. Two offers with the same service name can cover different systems, operating hours or responsibilities.

How liability differs from service performance

Clause 19 separates performance obligations from financial liability. Subject to the clause's exclusions and applicable law, the general cap per event or series of connected events is the greater of the fees paid in the preceding three months or \$25,000. Confidentiality, information security, privacy and the IP indemnity have a \$1 million cap per event or series of connected events and a \$2 million aggregate cap. 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.

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.

Continuity when an external event interrupts service

Clause 23 addresses force majeure separately from normal incident management. Performance is suspended to the extent a qualifying event causes delay or failure. The definition includes specified events outside reasonable control; it is not a blanket classification of every outage. If the delay exceeds 20 Business Days, the other party may terminate by written notice. The clause also requires payment for services to termination and the applicable Early Termination Payment. A continuity plan should cover operational recovery and the commercial consequences of prolonged interruption. Confirm the Schedule's exit calculation rather than assuming an externally caused outage creates a cost-free exit.

Responsibility across the delivery chain

The published terms permit subcontracting all or part of the Service Agreement without prior written customer consent. Confirm any separate notification obligations and negotiated conditions in the applicable agreement. Clause 27.5 nevertheless makes us liable for our subcontractors' acts and omissions to the same extent as for our employees. This differs from a third-party supplier contracted directly by the customer. Identify which arrangement applies to each dependency in the design. Where supplier identity, delivery location or change notification matters, request a documented supplier list and put any agreed notification or approval requirement in the Service Order; the general clause does not supply that visibility automatically.

Related

emPOWER Cloud

Public Cloud: Microsoft Azure

Azure Local

Disaster Recovery as a Service

Offsite Backup as a Service

Storage as a Service (Private S3)

Private and Public SaaS Backup

Connectivity hub

Managed Services hub

Microsoft Practice hub

Security hub

ISO 27001 certification

Data sovereignty and privacy

blueAPACHE Cloud case study

Archers case study

Honan Insurance case study
Healthcare and Aged Care industry page
Financial Services industry page
Service agreement
Home

Where is our data physically stored if we use emPOWER Cloud?

Our private-cloud offering includes Australian data centres. Confirm the agreed locations for primary data, replicas, backups and administrative access for your workload. Clause 18.3 addresses overseas transfers of Personal Information; read it alongside the agreed service scope and applicable privacy obligations.

What uptime does emPOWER Cloud publish?

The emPOWER Cloud brochure quotes 99.999 per cent uptime for cloud and 100 per cent for the all-flash HPE Primera storage component. These are separate component claims. Confirm measurement periods, exclusions, remedies and credits in the applicable Service Description, Schedule 3 and Service Order; the brochure figures alone do not establish those contractual details.

Is emPOWER Cloud ISO 27001 certified?

emPOWER Cloud Services (IaaS), emPOWER IT Continuity Services (DRaaS) and emPOWER Co-Location Services are all listed as in-scope services on our ISO/IEC 27001:2022 certificate 202507-118, issued by Sensiba Australia Pty Ltd and valid from 1 August 2025 to 1 August 2028. The certificate covers our information security management system; it does not certify the products or services themselves.

What hardware runs emPOWER Cloud?

The brochure identifies HPE Synergy compute modules, all-flash HPE Primera SSD arrays and HPE BladeSystem servers in a Tier 1 HPE reference architecture. Our February 2021 HPE GreenLake case study describes consuming infrastructure as a service. Confirm the current hardware and delivery model for the proposed deployment.

Which hypervisor does emPOWER Cloud use?

Ask directly if your workloads carry a hypervisor dependency or licensing implication.

How is emPOWER Cloud priced?

Consumption-based options are available. Where the Service Order specifies usage-based fees, the General Terms provide for monthly billing in arrears and rounding to whole units. Fixed fees and any Minimum Spend still apply as agreed. The portal can change technical capacity, but the agreement determines whether and when charges reduce.

Can we use our existing Microsoft 365 or Windows licences on emPOWER Cloud?

emPOWER Cloud is part of Microsoft's Qualified Multitenant Host (QMT) Program, which lets organisations use certain Microsoft 365 and Windows 11 licensing on our environment.

What exactly does the disaster recovery service commit to?

emPOWER IT Continuity Services (DRaaS) is limited by clause 3.17 of the General Terms and Conditions to restoring the Customer Data and Software that is the subject of the agreed Restore Time Objective and Recovery Point Objective set out in the Schedule. A workload with no agreed objectives has no DR commitment.

If data is lost and there was no backup obligation, what are you liable for?

Clause 19.4 excludes liability for loss of or damage to Customer Data unless a contracted backup or disaster-recovery obligation exists and is breached, with liability then limited to the specified restoration cost. This summary is subject to applicable law, non-excludable rights and the agreed terms. If no backup service is included, the customer must keep regular, complete backups.

Which compliance frameworks does the platform align to?

The cloud services are named within the scope of our ISO/IEC 27001:2022-certified information security management system. The brochure also references APRA CPS 234, NIST data-management controls and ASD Essential Eight Maturity Level 3. Request current assessment evidence, dates and scope for those positions during due diligence; they do not certify the customer's compliance.

Can emPOWER Cloud connect directly to Azure or AWS?

Yes. The emPOWER Network provides Azure ExpressRoute connections (Azure, SharePoint, Microsoft 365) and an AWS Direct Connect link, and emPOWER Connectivity offers direct public cloud connections with a secondary VPN-over-internet path for redundancy. This supports hybrid designs where some workloads stay on emPOWER Cloud and others run in public cloud.

What is emPOWER Cloud?

emPOWER Cloud is our private and hybrid Infrastructure-as-a-Service platform. The cloud services are named within the scope of our ISO/IEC 27001-certified information security management system; the certification does not certify individual products.

What services are included under your Cloud pillar?

The Cloud pillar includes emPOWER Cloud, Public Cloud - Microsoft Azure, Azure Local, Disaster Recovery as a Service, Offsite Backup as a Service, Private and Public SaaS Backup, and Storage as a Service (Private S3).

How is pricing structured for your Cloud services?

Consumption-based options are available. Where the Service Order specifies usage-based fees, they are billed monthly in arrears under the General Terms, subject to agreed fixed fees, Minimum Spend and term commitments. Confirm scale-down and billing conditions in your order.

Which countries does your Cloud service area cover?

Our published data-centre reach spans Australia, New Zealand, the United States, the United Kingdom and Singapore. Confirm availability and the hosting, backup and access locations for your specific cloud service.

Who is the target audience for your Cloud services?

The offering supports business workloads, with mid-market and enterprise positioning described in our HPE case study. Suitability for a particular organisation depends on workload, security, residency and contractual requirements.

Which other service pillars are related to your Cloud pillar?

The Cloud pillar is related to emPOWER Connectivity, the Microsoft Practice, and emPOWER Managed Services.

What infrastructure underpins emPOWER Cloud?

The emPOWER Cloud brochure describes Tier 1 HPE reference architecture using HPE Synergy compute modules, HPE Primera SSD storage and HPE BladeSystem servers. Confirm the current deployment hardware. ISO/IEC 27001 certification applies to the information security management system, not the hardware products.

How can I contact you about Cloud services?

You can contact our sales team by phone at 1800 248 749 (area served: AU) or via the contact page listed as the service channel.