

Microsoft Practice & Cloud Services | blueAPACHE

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

Details:

Key facts

Fact	Value
Practice name	Microsoft Practice
Solution areas	Modern Work; Infrastructure (Azure); Security; Data and AI
Partner status stated	Microsoft Solutions Partner across all four solution areas
Microsoft programme statuses	Tier 1 Cloud Solution Provider; SPLA hoster; Qualified Multitenant Hoster
Modern Work scope	Microsoft 365, Teams, Copilot, SharePoint, Intune and the wider Microsoft workplace ecosystem
Infrastructure scope	Azure infrastructure, migration and optimisation; Azure Local
Security scope	Microsoft's security platform aligned to Zero Trust principles; MDR integration with Microsoft Security, Microsoft Identity and Sentinel
Data and AI scope	Data platform modernisation, governance, analytics and reporting, AI readiness, process automation on Azure
Hosting programme	emPOWER Cloud is part of Microsoft's Qualified Multitenant Hoster (QMTH) Program for certain Microsoft 365 and Windows 11 licensing
Network to Microsoft	Azure ExpressRoute connectivity is described in the emPOWER Network brochure; Microsoft 365 connectivity requires separate design and eligibility checks
Voice	Microsoft Teams PSTN services and Direct Routing
Identity resilience	emPOWER Backup for Microsoft Entra ID, powered by Veeam, hosted on our private cloud within Australia
Third-party software definition	Microsoft is the example named in the General Terms and Conditions definition of Third Party Software

Contract schedules	Confirm the applicable schedules in the Service Order: Schedule 1 covers Professional Services, Schedule 10 software licensing and subscriptions, and Schedule 2 emPOWER Managed Services
--------------------	---

The three Microsoft programme statuses, and why they differ

Our Microsoft position has two distinct parts, and they are often conflated. The Solutions Partner designations across Modern Work, Infrastructure, Security and Data and AI are competency recognitions: they signal demonstrated customer success, certified technical capability and ongoing investment in skills. The programme statuses are commercial and licensing arrangements, and they are what actually determine how you can buy and where licences can run.

Status	What it permits
Tier 1 Cloud Solution Provider	Our partner page states this status. Confirm the subscription seller, billing arrangements, tenant administration and support responsibilities in your order
SPLA hoster	Our partner page states this hosting programme status. Confirm the eligible products, reporting and charging model, and applicable Microsoft terms for the proposed hosted service
Qualified Multitenant Hoster (QMTH)	The emPOWER Cloud brochure describes use of certain Microsoft 365 and Windows 11 licences in its environment; eligibility depends on the specific subscription, workload and applicable Microsoft terms

These programme statements describe potential procurement and hosting arrangements. They do not establish that every product or existing licence is eligible. Confirm the current programme terms, subscription entitlements, commercial route and support scope for your proposed deployment.

Speak with our team about the Microsoft designations, specialisations and technical certifications relevant to your requirements.

What the pillar covers

Our stated capability list is: Microsoft 365 and Modern Work solutions; Azure infrastructure, migration and optimisation; Microsoft Security solutions aligned to Zero Trust principles; data, analytics and AI capabilities on Azure; ongoing governance, optimisation and operational management; and certified Microsoft expertise across the four solution areas.

Solution area	Capability
Modern Work	Help people work productively and securely through Microsoft 365, Teams, Copilot, SharePoint, Intune and the broader Microsoft workplace ecosystem
Infrastructure (Azure)	Build resilient, scalable cloud foundations through Azure infrastructure, migration and optimisation

	services
Security	Protect identities, endpoints, applications, data and cloud environments through Microsoft's security platform and Zero Trust principles
Data and AI	Turn information into insight and prepare for AI-driven innovation

The Data and AI Practice is described in more detail: modernising data platforms, improving governance and visibility, unlocking insight through analytics and reporting, accelerating AI readiness and adoption, automating processes and operations, and enabling data-driven decision-making, on the premise that AI only delivers value when built on trusted, accessible and well-governed data.

Services in this pillar

The Microsoft-specific services below are published under other hubs and are the practice's delivery vehicles.

Public Cloud: Microsoft Azure

Azure public cloud for organisations that need scalable infrastructure and modern cloud capability, with our support across planning, migration and operations. The emPOWER Network's ExpressRoute connections give Azure workloads a private path from the customer's sites, and emPOWER Connectivity offers a direct Azure connection with a VPN-over-internet fallback. This is the Infrastructure solution area in practice.

Azure Local

Azure-based management and services extended to on-premise workloads where local performance, control or data residency requirements apply. Discuss the Azure management services, supported workloads and integration boundaries for your on-premise, private and public infrastructure; the practice overview does not promise one control plane for every environment.

Microsoft Teams

Teams chat, meetings and calling, with us providing Teams PSTN services and Direct Routing on the emPOWER Network. The Archers case describes Teams calling replacing legacy VoIP/PBX. Berry Street selected Teams telephony after an RFP; that migration was still in progress when its historical case was written.

Private and Public SaaS Backup

Independent backup for Microsoft 365 and other SaaS data, plus emPOWER Backup for Microsoft Entra ID: automated, Veeam-powered backup of users, groups, roles and role assignments, application registrations and directory configuration, with granular restore, delivered as a fully managed service on our private cloud within Australia. Our rationale is the shared responsibility model: Microsoft secures the Entra ID platform, the customer remains responsible for its identity data and configuration, and native recovery is limited.

Managed Detection and Response

emPOWER MDR integrates with Microsoft Security, Microsoft Identity and Microsoft Sentinel, and its identity threat detection targets the credential theft, adversary-in-the-middle, mailbox-rule and rogue OAuth application attacks that Microsoft 365 tenants face. This is the Security solution area delivered as a 24/7 managed service.

How it is delivered

Advisory and design. The practice describes assessment, architecture, migration and optimisation capabilities. Agree the engagement scope and applicable schedules in the Service Order. The Archers case records a security assessment for future AI capabilities including Microsoft Copilot within that client's managed services engagement; it is an example rather than a standard project specification. Under General Terms v3.6, Professional Services are excluded from the default 36-month Minimum Service Period. Clause 13.10 grants the customer and its Affiliates a worldwide, royalty-free, non-exclusive licence to use, copy and adapt Deliverables internally during the Service Period upon full payment of the relevant fees, expenses and Taxes. Check the applicable agreement and any negotiated continuing rights.

Migration and modernisation. Azure migration, Teams telephony migration, Intune device management and Entra ID configuration are delivered as projects. In Archers' case, Intune provided zero-touch provisioning of new hardware and a standardised desktop experience, and Teams calling replaced an unreliable legacy VoIP/PBX. Berry Street's Teams telephony migration followed a second RFP that we won after the initial managed services appointment.

Licensing. Microsoft is the example named in the General Terms and Conditions definition of Third Party Software: software licensed to us for onward licensing to clients, provided the client enters into an agreement directly with the licensor. The customer is bound by Microsoft's terms whether or not they have been brought to its attention, must provide evidence of properly licensed and paid software within 5 Business Days of a written request under clause 13.7. Clause 19.5 permits retrospective licence fees where use is unauthorised or exceeds permitted use; an audit alone does not establish that liability. Microsoft price changes can be passed through proportionally under clause 12.5 from the date Microsoft changes its charges.

Ongoing management. Ongoing managed services and MDR can be specified alongside Microsoft projects. Confirm the ordered services, covered systems, monitoring, reporting and response responsibilities. A Microsoft deployment does not automatically include either service. The managed-services brochure describes help desk, patching and monitoring capabilities; reporting within 5 Business Days of month end and 6-monthly reviews are described in the general terms, subject to the applicable agreement.

Customer Zero. The Managed Services and Security pages describe using our own operating environment to prove architecture and controls. Separately, the Archers case describes access to experience across application virtualisation, MDR and Microsoft platforms. These are distinct examples of internal practice and customer experience.

Support and service levels

Published capabilities. The managed-services brochure describes unlimited 24/7 help desk support, with Australian-based staff in business hours. The network and MDR materials describe their respective monitoring and response capabilities. Confirm which Microsoft workloads, integrations, operating hours and response actions your Service Description includes; connectivity to a workload alone does not establish that it is managed or protected by MDR.

Response and resolution targets, as elsewhere in the portfolio, are set per customer in the priority and escalation matrix and are not Service Levels unless written under that heading in the Service Description.

Contract points specific to Microsoft services. Where Microsoft, as licensor, requires it, we may have to terminate the affected part of a service if the customer breaches Microsoft's terms, without liability. Under clause 3.22, if the customer does not accept the licensor's click-through terms we may be unable to provide certain services. General Terms v3.6 restrict processing of personal data subject to the GDPR. Establish the data and legal requirements for your proposed service and agree any required variation; nationality alone does not determine GDPR applicability.

How it integrates with the other pillars

Cloud. QMTH hosting of Microsoft licences on emPOWER Cloud, Azure and Azure Local services, ExpressRoute, and Entra ID backup on our private cloud. See the Cloud hub .

Collaboration. Microsoft Teams calling, PSTN and Direct Routing, and the Modern Work solution area. See the Collaboration hub .

Security. Microsoft Security, Microsoft Identity and Sentinel integration within MDR; Zero Trust-aligned Microsoft security design; identity threat detection for Microsoft 365. See the Security hub .

Connectivity. ExpressRoute and direct Azure connections on the emPOWER Network; IX peering cited for lower latency to Microsoft 365 and Teams. See the Connectivity hub .

Managed Services. Ongoing operation of Microsoft 365, Intune and Azure estates under the help desk and lifecycle management model. See the Managed Services hub .

Procurement. Microsoft licensing and subscription arrangements, with the applicable Schedule 10 scope, transaction route and hosted licence eligibility confirmed in your order. See the Procurement hub .

Our client outcomes

Customer	Microsoft element	Stated outcome
Archers The Strata Professionals (2026)	Microsoft Teams calling replacing legacy VoIP/PBX; Microsoft Intune zero-touch provisioning; security assessment for Microsoft Copilot readiness; retirement of end-of-life Windows Server 2012	Client states significant licensing savings and easier cross-channel and remote communication; standardised desktop experience; AI readiness assessed
Berry Street (historical engagement from 2020)	Selected via RFP to migrate an end-of-life on-premises voice solution to Microsoft Teams telephony; 1400 staff mobilised to work from home	Transition delivered on time and within budget; Teams migration in progress at the time of writing
Honan Insurance (c. 2020-2021)	Citrix transformation and cloud migration supporting remote work	Staff able to work remotely with no impact on performance during COVID-19

Separating Microsoft entitlements from managed work

Distinguish licence entitlements, subscription or tenant ownership and the work we will perform. Modern Work, Azure, Security and Data & AI can involve different administrators, data locations and consumption models. Record covered workloads and who authorises consumption or configuration changes. Partner status supports a capability statement, but does not specify customer licence

eligibility or operational support scope. Keep applicable vendor terms with the Service Description so both sides of the arrangement can be checked.

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.

Responsibility across the delivery chain

The published terms allow us to subcontract all or part of the Service Agreement without customer consent or a notification requirement. 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.

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.

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 of receiving that determination. Missing the required windows can waive the right to correction, subject to the fraud exception. We may charge interest on overdue amounts at the published margin of 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.

How liability differs from service performance

Clause 19 separates performance obligations from financial liability. Under General Terms v3.6 clause 19.3, subject to clauses 19.1, 19.2 and 19.4 and applicable law, the per-single-claim limit is the greater of amounts paid under the agreement in the three months before the claim first arose or \$25,000. Clause 19.4(e) specifies \$1 million per event or series of connected events and \$2 million in aggregate for breaches of clauses 16, 17, 18 or 20. Confirm the version and variations applying to your agreement. 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.

Related

Public Cloud: Microsoft Azure

Azure Local

Microsoft Teams

Private and Public SaaS Backup

Managed Detection and Response

Cloud hub

Collaboration hub

Security hub

Managed Services hub

Procurement hub

Consulting and Advisory hub

Our partners

Vendor partner record

Archers case study

Honan Insurance case study

Professional Services industry page

Service agreement

Support

Contact

What Microsoft partner status do you hold?

Our Microsoft Practice page describes Solutions Partner expertise across Modern Work, Infrastructure, Security, and Data and AI. Our partner page states Tier 1 Cloud Solution Provider, SPLA hoster and Qualified Multitenant Hoster status. Confirm current programme and product eligibility for your proposed purchase.

What does Tier 1 Cloud Solution Provider mean for us?

Our partner page states Tier 1 Cloud Solution Provider status. For your subscriptions, confirm the selling and billing entity, tenant administration, support path and licensing advice in the order. Programme status alone does not set every customer responsibility.

What is SPLA and why does it matter?

Our partner page identifies blueAPACHE as an SPLA hoster. Ask which Microsoft products and licensing model apply to the proposed hosted workload, including charging and reporting requirements. SPLA hosting, cloud subscriptions and bringing eligible licences are distinct arrangements; eligibility must be checked for the specific service.

Can we run our Microsoft 365 or Windows licences on your cloud?

The emPOWER Cloud brochure describes participation in Microsoft's Qualified Multitenant Hosted (QMTH) Program and use of certain Microsoft 365 and Windows 11 licences in that environment. Confirm current eligibility for your subscriptions and workloads before planning licence portability.

Do you provide Teams calling?

Yes. The emPOWER Network offers Microsoft Teams PSTN services and Direct Routing, delivered on our own MPLS core with QoS prioritisation for voice. Teams calling replaced legacy PBX systems in the Archers engagement and was selected for Berry Street after an RFP. Teams has its own service page under the Collaboration hub.

How do you connect us to Azure and Microsoft 365?

The emPOWER Network and Connectivity brochures describe Azure ExpressRoute/direct connectivity and a VPN-over-internet secondary path. Microsoft recommends internet connectivity for most Microsoft 365 scenarios; ExpressRoute for Microsoft 365 requires Microsoft authorisation and specific routing design. Confirm the Azure and Microsoft 365 paths separately. The emPOWER Internet brochure describes IX peering, but this is not a universal latency guarantee.

What does the Entra ID backup service cover?

Users and groups, roles and role assignments, application registrations, and directory and access configurations, backed up automatically using Veeam and stored on our private cloud within Australia, with granular restore of individual components. We position it against accidental or malicious deletion, misconfiguration and cyber incidents that disrupt authentication.

Is Microsoft security part of your MDR?

Yes. emPOWER MDR names Microsoft Security, Microsoft Identity and Microsoft Sentinel among its supported integrations, and its identity threat detection focuses on credential theft, adversary-in-the-middle MFA bypass, shadow mailbox rules, rogue OAuth applications and session hijacking, all of which are Microsoft 365 tenant attack patterns. The Microsoft Practice describes its security work as aligned to Zero Trust principles.

Do you help with Copilot and AI readiness?

The Microsoft Practice describes AI readiness, data governance, analytics and adoption capabilities. The Archers case is one documented example: a security assessment for future AI capabilities including Microsoft Copilot. Agree the assessment outputs and implementation scope for your organisation.

How are Microsoft projects contracted?

Confirm the applicable schedules and scope in your Service Order. The published terms describe Professional Services in Schedule 1, software licensing and subscriptions in Schedule 10, and emPOWER Managed Services in Schedule 2. Professional Services are excluded from the default 36-month Minimum Service Period. Clause 13.10's internal-use Deliverables licence for the customer and its Affiliates applies upon full payment of the relevant fees, expenses and Taxes and lasts during the Service Period, subject to the applicable agreement and variations.

Can Microsoft price changes be passed on to us?

Yes. Clause 12.5 of the General Terms and Conditions allows us to vary fees by the same proportion when a third-party licensor such as Microsoft changes its charges, including exchange-rate-driven changes, effective from the date of the licensor's change and without a signed Variation.

Is there a customer case study for an Azure migration?

The Microsoft elements evidenced in case studies are Teams calling, Intune and Copilot readiness (Archers), Teams telephony (Berry Street) and Citrix and cloud migration (Honan Insurance).

What is your Microsoft Practice?

Our Microsoft Practice provides Microsoft expertise across Modern Work, Infrastructure (Azure), Security and Data & AI, helping organisations maximise value from Microsoft technologies through one trusted partner.

What areas does the Microsoft Practice help modernise?

The Microsoft Practice helps organisations modernise Microsoft 365, Azure, security, and Data & AI, backed by our certified Microsoft Solutions Partner expertise.

Who provides the Microsoft Practice service and where is it offered?

blueAPACHE provides the Microsoft Practice in Australia. Discuss delivery requirements for your locations and workloads with our team.

How does Microsoft technology integrate with emPOWER Cloud?

The emPOWER Cloud brochure describes Qualified Multitenant Host participation and use of certain Microsoft 365 and Windows 11 licences in its environment. Confirm eligibility against the applicable Microsoft terms for your subscription and workload. Azure ExpressRoute connectivity is described separately in the network materials.

What Microsoft 365 and Teams capabilities are available through emPOWER Cloud?

The emPOWER Network materials describe Microsoft Teams PSTN services and Direct Routing. Azure ExpressRoute connectivity is also available, but Microsoft recommends internet connectivity for most Microsoft 365 scenarios; Microsoft 365 ExpressRoute requires authorisation and specific routing design. Confirm calling, licensing and connectivity scope for your environment.

How do you handle identity and access management for Microsoft environments?

The Microsoft Practice describes identity protection through Microsoft's security platform and Zero Trust principles. Separately, emPOWER Backup for Microsoft Entra ID protects identity data and configuration. That backup service does not by itself establish the identity and access management architecture of an emPOWER Cloud deployment; agree the required integration in your design.

What is emPOWER Backup for Microsoft Entra ID?

emPOWER Backup for Microsoft Entra ID is a specialized service, powered by Veeam, that delivers automated backup and recovery specifically for Microsoft Entra ID identity data. It protects critical identity components including users, groups, roles, role assignments, application registrations, and directory configurations, is delivered as a fully managed service on our private cloud infrastructure within Australia, and provides granular recovery capabilities to address the limited native recovery capabilities of Microsoft Entra ID.

How is Microsoft security technology used in your Managed Detection and Response (MDR) service?

Microsoft security integration, specifically Microsoft Security, is central to our emPOWER Managed Detection and Response (MDR) capabilities, supporting threat detection and monitoring.