

SaaS Backup Services | blueAPACHE

Canonical: <https://www.blueapache.com/services/private-and-public-saas-backup>

Details:

Summary

Private and Public SaaS Backup is our managed backup service for data held in cloud applications, giving organisations an independent copy and a recovery path that does not depend on the retention built into each SaaS platform. Our emPOWER Backup for Microsoft Entra ID brochure describes that named product as delivered on our private cloud within Australia. Confirm the hosting, protected applications and contract documents for your selected SaaS backup service. The commercial guidance below summarises General Terms and Conditions v3.6; the version, Schedule, Service Order and variations agreed with you govern your engagement.

Key facts

Label	Value
Service	Private and Public SaaS Backup, emPOWER Cloud pillar
Purpose	Independent backup for cloud and SaaS data beyond the retention and recovery options built into individual platforms
Named product published	emPOWER Backup for Microsoft Entra ID, powered by Veeam, protecting users, groups, roles, application registrations and directory configurations
Entra ID product delivery	The Entra ID brochure describes private cloud delivery, identity data stored within Australia and a browser-based experience
Backup obligation	Run backup software at agreed intervals; re-run after fixing the root cause of any reported failure (clause 3.14)
Retention, frequency and recovery targets	Confirm the values for your service in the applicable Schedule and Service Order; the Entra ID brochure does not specify them
Data-loss liability	Clause 19.4(a) distinguishes whether a backup or disaster recovery obligation exists and is breached, subject to clauses 19.1, 19.2 and applicable law
Contracted backup or DR obligation breached	Clause 19.4(a)(ii) limits liability to restoration cost to the applicable recovery point, subject to clauses 19.1, 19.2 and applicable law

Certification scope	Check the current certificate scope against the selected service, delivery entities and locations; an ISMS certificate does not itself certify every backup product
Default Minimum Service Period under v3.6	36 months from the Service Commencement Date, except Professional Services or where the Service Description or Service Order states otherwise

What is included

The service adds an independent, blueAPACHE-held copy to whatever the SaaS vendor retains natively.

The emPOWER Backup for Microsoft Entra ID brochure describes automated, scheduled backup of Entra ID users and groups, roles and role assignments, application registrations, and directory and access configurations, with granular recovery of individual identity components, a browser-based SaaS-like experience, and identity data stored on our private cloud within Australia. It is fully managed: operated, secured and supported end to end by us, and delivered as part of the managed services framework.

Contractually, where the Schedule includes backups, clause 3.14 obliges blueAPACHE to run the backup software at the agreed intervals and to re-run after addressing the root cause of any failure the software reports. Restoration returns the version of Customer Data that existed at the time of the relevant backup.

What is not included

Confirm the supported applications and objects before ordering, including any Microsoft 365 mailboxes, SharePoint, OneDrive or third-party SaaS data you need protected. Entra ID identity backup does not by itself establish coverage of those application contents.

How it is delivered

Agree the onboarding tasks, access, monitoring, documentation and reporting for the selected service. Where Transition In Services apply, clause 8 addresses the agreed transition arrangements. For Entra ID, scheduled, automated backups run by us with recovery initiated through a browser-based interface, granular to individual identity objects. Customers must maintain the SaaS licences and administrative access that let us perform the service, and must promptly report any suspected security compromise (clauses 7.1 and 3.19).

Commercial model

Confirm the pricing unit and any Minimum Spend in your Service Order. Under clause 12, unless the Service Order states otherwise, fixed Fee Services are billed monthly in advance and the specified usage-based charging is monthly in arrears. Direct debit is the default payment method, and GST is additional. Where the SaaS vendor or Veeam changes its charges to us, clause 12.5 allows the fee to be varied in the same proportion without a signed Variation.

Support and service levels

Service Levels are only those stated under the "Service Level" heading in the Service Description, measured by our tools, and subject to the Reasonable Excuse carve-out, which includes outages caused by third-party software used by us. Monthly reports arrive within five Business Days of month end, and the parties review the Services every six months. Check the applicable Service Description, Schedule and Service Order for any service credits, claim conditions and remedies. The definition of a Service Level does not remove other contractual obligations.

Related services

Related options include Offsite Backup as a Service, Disaster Recovery as a Service and Storage as a Service (Private S3). Confirm their workload coverage, retention and configuration separately. Under clause 3.17, contracted DRaaS is limited to restoring the Customer Data and Software subject to the agreed Restore Time Objective and Recovery Point Objective in the relevant Schedule. Human Risk Management, Managed Detection and Response and Microsoft Practice services may complement a backup design; they are not automatically included.

Buying questions

Contract term and renewal. Under v3.6 clause 2.6, the default Minimum Service Period is 36 months from the Service Commencement Date, except Professional Services or where the Service Description or Service Order states otherwise. Clause 2.8 provides a Written Notice route before expiry; clause 2.10 also permits renewal variations through emails, faxes or continued use. The three-month holdover at full list price without Service Levels applies when no clause 2.8 notice is given and the customer continues to access or use a Service after expiry.

Termination. Clause 24.1 gives the customer termination rights for a breach not remedied within 20 Business Days of written notice specifying it, and for blueAPACHE insolvency or ceasing business. Clause 24.2 includes blueAPACHE rights for non-payment not remedied within five Business Days of written notice specifying it, specified breaches not remedied within 20 Business Days of such notice, and the listed insolvency, business-cessation and control events. Confirm the required termination notice and any Early Termination Payment, Minimum Spend or remaining fees under the applicable clauses and Schedule.

Scope. Name every SaaS platform, tenant and data type to be protected, the backup frequency and retention period, and the restore granularity. Check the complete agreement for backup and disaster recovery obligations. Clause 17.2 ties its backup duty to the Service Order, while clauses 3.14 and 3.17 address express Schedule commitments. Data-loss liability under clause 19.4(a) depends on those obligations and is subject to clauses 19.1, 19.2 and applicable law.

Third-party terms. Under clauses 3.20 to 3.24 the customer is bound by the SaaS vendor's and backup software licensor's terms whether or not they have been shown, and we may have to terminate that part of the Service if the customer breaches them.

Exit. Clause 9.1 requires the customer to take its own copy before expiry and addresses deletion of Customer Software and Customer Data from our environment at the end of the Service Period. Agree export format, timing and any additional exit assistance; do not assume deletion waits for confirmation that you have copied the data.

Data protection. Mutual Privacy Act compliance, 24-hour eligible data breach notification, standing overseas transfer consent in clause 18.3, and the customer's warranty that no GDPR-regulated personal data is provided (clause 18.6).

Defining the SaaS data boundary

Specify applications, tenants, users and data types covered. Record retention and restore requirements for deleted users, changed permissions and records needed after account closure. Platform availability differs from recovery of a particular item. Identify restore authority and application validation. The service name does not establish coverage of every SaaS product or every object within a supported product.

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.

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.

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.

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.

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 notice of the amount we determine is correct. 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.

Related

Cloud pillar hub

Microsoft Practice hub

emPOWER Cloud

Offsite Backup as a Service

Disaster Recovery as a Service

Storage as a Service (Private S3)

Managed Detection and Response

Human Risk Management

Case study: Archers The Strata Professionals

Industry: Professional services

Industry: Financial services

Service Agreement terms

Support

Contact blueAPACHE

Why consider independent Entra ID backup?

Our Entra ID brochure explains that customers remain responsible for protecting identity data, configurations and policies and describes independent backup as a way to improve identity resilience. Check the native recovery features, retention limits and any separately purchased backup services for each application before selecting additional protection.

Which SaaS platforms can we back up?

emPOWER Backup for Microsoft Entra ID is documented in detail.

What does emPOWER Backup for Microsoft Entra ID protect?

Users and groups, roles and role assignments, application registrations, and directory and access configurations, with granular restore of individual identity components. It is powered by Veeam and runs on our private cloud within Australia.

How long is SaaS backup data retained?

As agreed in your Schedule and Service Order.

Is SaaS backup the same as disaster recovery?

SaaS backup and disaster recovery address different recovery needs. Confirm which data and granular restore options your backup includes. Under clause 3.17, DRaaS restoration covers only Customer Data and Software subject to the agreed Restore Time Objective and Recovery Point Objective in the relevant Schedule.

What if a SaaS platform is not listed in our agreement?

Confirm coverage against the complete Service Agreement. Clause 17.2 addresses backup to the extent stated in the Service Order, and clauses 3.14 and 3.17 address express backup and DR Schedule commitments. Where backup is not included, clause 3.15 requires customer backups and duplicate copies. Clause 19.4(a) governs data-loss liability subject to clauses 19.1, 19.2 and applicable law.

What happens if a backup job fails?

Under clause 3.14, where the backup software records a failure, we must address the root cause and re-run the backup until success is recorded. Ask how completion status is reported to you.

Who supports restore requests?

The Entra ID brochure describes that product as operated, secured and supported end to end by us. Confirm the support channel, hours, restore authorisation and response commitments for your service; general platform or managed-service support hours do not by themselves establish your restore SLA.

How long is the contract and how does it end?

Under v3.6, the default initial Minimum Service Period is 36 months from the Service Commencement Date, except Professional Services or where the Service Description or Service Order states otherwise. Check clauses 2.8–2.10 for notice, renewal and continued-use holdover, and the applicable Schedule for early-exit charges. Take your data copy before expiry; clause 9.1 does not make deletion conditional on you completing that copy.

Is the service certified?

Our ISO/IEC 27001:2022 certificate describes the scope of the information security management system. Ask for the current certificate and confirm how its scope relates to your selected service, delivery entities and locations. The Entra ID brochure describes managed private cloud delivery within Australia; that does not establish separate product certification for every SaaS backup offer.

What is your Private and Public SaaS Backup service?

It is a service providing independent backup for cloud and SaaS data that improves recoverability beyond the retention and recovery options built into individual platforms. It is designed to protect cloud application data with independent backup and recovery across modern SaaS environments.

Who provides the Private and Public SaaS Backup service?

The service is provided by us.

What category and service type does this offering fall under?

The service falls under the 'Cloud' category, with a service type of 'Cloud, backup and recovery'.

Where is this SaaS Backup service available?

Our service page identifies Australia as the area served. Confirm availability and delivery arrangements for your organisation and locations.

What does the Entra ID backup product's delivery experience include?

The emPOWER Backup for Microsoft Entra ID brochure describes a fully managed, browser-based service with automated scheduled protection of identity objects and configurations and granular recovery of individual components. Confirm the scope of other SaaS backup products separately.

Where is Entra ID backup data stored, and how should certification be checked?

The Entra ID brochure describes identity data stored on our private cloud within Australia. Ask for the current ISO/IEC 27001 certificate and confirm the ISMS scope against the selected service, delivery entities and locations; it does not establish separate certification of every backup product.

How does Entra ID backup fit into broader managed services?

The Entra ID brochure describes the product as part of our managed services framework and operated, secured and supported end to end by us. Confirm the support hours, restore process and any other services included in your agreement.