

# Offsite Backup as a Service | blueAPACHE

Canonical: <https://www.blueapache.com/services/offsite-backup-as-a-service>

## Details:

### Summary

Offsite Backup as a Service keeps an independent copy of critical data away from primary infrastructure to support recovery and business continuity. Separation can reduce exposure to a primary-site disruption, but recovery also depends on the backup design, access controls and restore validation. Confirm the platform, storage and processing locations, backup intervals, retention and protected data in your Service Order and applicable service documents. This page explains the contractual boundaries in General Terms v3.6; confirm the version governing your order.

### Key facts

| Label                          | Value                                                                                                                                                                                    |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Service                        | Offsite Backup as a Service, part of the emPOWER Cloud pillar                                                                                                                            |
| What it does                   | Maintains protected copies of critical data outside the primary environment, with automated offsite backups                                                                              |
| Backup obligation              | Where the Schedule includes backups: run backup software at agreed intervals and re-run after addressing the root cause of any reported failure (clause 3.14)                            |
| What a restore returns         | Only the version of Customer Data that existed at the time of the relevant backup, even if already corrupted                                                                             |
| Backup frequency and retention | Confirm the values for your protected data in the applicable service documents                                                                                                           |
| Backup locations and platform  | Confirm the target platform, storage, processing and support locations, and any required certification scope for your configuration                                                      |
| Data-loss liability            | Clause 19.4(a) links exclusions and restoration-cost limits to the relevant backup/DR obligation and breach; subject to clauses 19.1 and 19.2, applicable law and the complete agreement |
| Default contract term in v3.6  | 36 months except Professional Services, unless the Service Description or Service Order specifies otherwise                                                                              |

## What is included

Agree the backup target and network path in the solution design. Related emPOWER Cloud and Connectivity capabilities do not establish the platform or path used by every Offsite Backup order.

Contractually, where the Schedule expressly states that a Service includes backups of Customer Data, clause 3.14 of the general terms sets the obligation: we run the backup software at the agreed intervals, and if the software records a failure we must address the root cause and re-run until a successful completion is recorded. The obligation is a process obligation, not an outcome guarantee. Clause 17.3 adds that we must back up Customer Data "to the extent set out in the Service Order" and in accordance with any applicable Service Levels.

## What is not included

Clause 17.3 is explicit: if backups are not set out in the Service Order, "blueAPACHE has no obligation in this respect", and clause 3.15 then requires the customer to take regular and complete backups itself in accordance with industry best practice and to keep duplicate copies of all data provided to us.

Offsite backup is not disaster recovery. It preserves a copy of data; it does not commit to restoring a running service within a Restore Time Objective. That is the separate emPOWER IT Continuity Services (DRaaS) product. Confirm whether Microsoft 365 or other SaaS workloads are included; Private and Public SaaS Backup is a related offering to assess. Clause 3.14 specifies action on reported backup failures, but it does not by itself determine every liability or performance question involving an undetected failure. Read the complete backup, care and service-level obligations. Agree backup frequency, retention, restore validation and any recovery objectives for the proposed service.

## Who it is for

Organisations whose backup currently sits alongside production and would be lost with it; organisations replacing tape or ad hoc scripts with a managed, monitored service; and organisations that need backups held in Australia under Australian jurisdiction. An undated Storage-as-a-Service case study describes an unnamed pathology provider with hundreds of clinics replacing tape and protecting data across three data centres. The source says the provider needed to retain records for at least ten years. This is a storage example, not evidence of the exact Offsite Backup architecture or a retention rule for every healthcare customer.

## How it is delivered

Clause 8 of General Terms v3.6 describes Transition In due diligence, monitoring setup where applicable, support documentation and agreement on meetings and reporting. Confirm the protected data, backup intervals and specific onboarding deliverables in the applicable service documents.

In operation, we run the backup software at those intervals and monitor completion records. Monthly reports on performance against Service Levels are provided within five Business Days of month end (clause 4.9). Customers must give blueAPACHE 24x7 remote access to the relevant components (clause 7.1) and keep Customer Software at the current or previous release level, because customer-side failures are Reasonable Excuses that disapply Service Levels.

## Commercial model

The service is contracted on a Service Order. Fixed fees are invoiced monthly in advance; usage-based charges, which for a storage-backed service commonly means capacity consumed, are

invoiced monthly in arrears subject to any Minimum Spend, and usage may be rounded up to the nearest whole unit (clause 12.2). Direct debit is the default payment method, GST is additional, and third-party cost changes may be passed through in proportion under clause 12.5. Request a quote identifying the billing units, minimum commitments and restore or exit charges for your scope.

## **Support and service levels**

Customers holding emPOWER Managed Services also receive its unlimited 24/7 help desk, Australian-based in business hours (0700 to 1900 AEST/AEDT on Business Days under the general terms) and follow-the-sun after hours. Customers holding only emPOWER Connectivity have a 7am to 7pm business-day service desk with 24x7 network monitoring; which desk applies should be confirmed at contract.

Service Levels are only those stated under the "Service Level" heading in the Service Description, are measured with our tools, and are subject to the Reasonable Excuse carve-out. The general terms contain no service credit regime; remedies sit in the Schedule. Clause 3.10 requires best efforts to carry out scheduled maintenance within the Schedule windows, or at other times with at least three Business Days' prior notice, and with minimum disruption to the customer's business. Emergency provisions are separate.

## **Related services**

Disaster Recovery as a Service adds a Restore Time Objective on top of the backup copy. Private and Public SaaS Backup covers SaaS platforms. Storage as a Service (Private S3) offers storage and immutability options; the undated pathology case illustrates one deployment. emPOWER Cloud and emPOWER Backup for Microsoft Entra ID are related capabilities. Confirm hosting, interoperability, protected workloads and any Entra ID backup requirements in the proposed design rather than assuming these offerings share one platform or are included together.

## **Buying questions**

Contract term and renewal. General Terms v3.6 provide a 36-month default Minimum Service Period from the Service Commencement Date, except Professional Services and where the Service Description or Service Order specifies otherwise. Confirm the version and negotiated terms applicable to your order. Clause 2.8 addresses written notice before the Service Period ends. Under clause 2.10, renewal may also be agreed by email or fax with or without a signature, or by continued use. If the customer gives no notice under clause 2.8 but continues to access or use services after the period ends, clause 2.9 extends all Services on that agreement for three months at the then-current full list price, with defined Service Levels not applying during that period.

Termination. Customer termination for unremedied breach after 20 Business Days' notice, or blueAPACHE insolvency or ceasing business (clause 24.1). blueAPACHE termination or suspension for non-payment after five Business Days' notice, specified breaches after 20 Business Days, insolvency or change of control (clause 24.2). Any Early Termination Payment depends on the termination ground, applicable Schedule and complete agreement.

Record protected data, backup intervals and retention in the service documents, and reconcile them with the complete agreement and any variations. Clause 19.4(a) addresses liability for loss of or damage to Customer Data: it excludes that liability where no relevant backup or disaster recovery obligation exists, and where such an obligation exists and is breached limits it to the specified restoration cost. Read it with clauses 19.1 and 19.2, applicable law and the complete agreement.

Exit. We delete Customer Data from our environment at the end of the Service Period at no cost and the customer must take their own copy first (clause 9.1). Clause 17.4 specifies return of Customer Records within ten Business Days; it does not establish a universal backup-export window. Check the applicable Schedule and Service Order and agree timing, format and access for exporting backup sets. Data protection. Privacy Act compliance and 24-hour eligible data breach notification are mutual (clause 18). Clause 18.3 carries a standing consent to transfer Personal Information to listed overseas destinations, while our data sovereignty statement says cross-border transfer does not occur by default; ask which applies to backup data.

## **Distinguishing a backup job from a recoverable workload**

A successful backup job does not establish that the application was healthy when copied. Identify protected data, intervals, retention and restore validation. Record who checks application consistency and dependencies such as identity. Where a time-bound return to service is needed, establish whether the separate recovery service and agreed objectives are required rather than assuming offsite copies provide the same commitment.

### ***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.

### ***How liability differs from service performance***

Clause 19 separates performance obligations from financial liability. Under General Terms v3.6, the general cap per Claim is the greater of amounts paid under the Service Agreement in the three months before the Claim first arose and \$25,000, subject to clauses 19.1, 19.2 and 19.4 and applicable law. The specified confidentiality, information-security, privacy and IP-indemnity liabilities have a \$1 million cap per event or connected series of 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.

### ***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 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.

### **Related**

Cloud pillar hub

emPOWER Cloud

Disaster Recovery as a Service

Private and Public SaaS Backup

Storage as a Service (Private S3)

Advanced Infrastructure Managed Services

Managed Services pillar hub

Case study: Archers The Strata Professionals

Industry: Healthcare and aged care

Industry: Professional services

Service Agreement terms

Support

Contact blueAPACHE

### ***How often are backups taken?***

At the intervals agreed in your Schedule and Service Order.

### ***What happens if a backup fails?***

Under clause 3.14 of the general terms, if the backup software records a failure, we must address the root cause and re-run the backup until the software records success. The obligation is to run the software and act on reported failures, not a guarantee that every copy is restorable.

### ***How far back does a restore take us?***

To the version of Customer Data that existed at the time of the relevant backup. If that data was already corrupted or damaged at the time of the backup, the same corrupted data is restored.

### ***Is our backup data held in Australia?***

Our data sovereignty statement says customer data is stored and processed in Australian-based data centres and remains subject to Australian legal jurisdiction. Clause 18.3 of the general terms separately records a standing consent for overseas transfer of Personal Information, so confirm the position for your backup sets on the Service Order.

### ***Does this back up Microsoft 365 or other SaaS platforms?***

Confirm the SaaS workloads and data types included in your backup scope. Private and Public SaaS Backup is a related offering; the service names alone do not establish inclusion or exclusion under your order.

### ***Is offsite backup the same as disaster recovery?***

No. Offsite backup preserves an independent copy of data. Disaster Recovery as a Service (emPOWER IT Continuity Services) commits to restoring Customer Data and Software within an agreed Restore Time Objective. Many organisations hold the first and assume they have the second.

### ***What are you liable for if backed-up data is lost?***

Clause 19.4(a) addresses liability for loss of or damage to Customer Data: it excludes that liability where no relevant backup or disaster recovery obligation exists, and where such an obligation exists and is breached limits it to the specified restoration cost. Read it with clauses 19.1 and 19.2, applicable law and the complete agreement.

### ***What must we do on our side?***

Provide 24x7 remote access to the systems being backed up, keep Customer Software at the current or previous release level, ensure it is properly licensed, and notify us promptly of any suspected security compromise (clauses 7.1 and 3.19). Failures caused by customer-side actions are Reasonable Excuses.

### ***How is the service priced?***

On a Service Order with fixed fees monthly in advance and any usage components monthly in arrears; usage may be rounded up to the nearest whole unit. Request a quote for your data volumes, retention, restore requirements and any exit charges.

### ***How long is the contract?***

General Terms v3.6 provide a 36-month default Minimum Service Period from the Service Commencement Date, except Professional Services and where the Service Description or Service Order specifies otherwise. Confirm the version and negotiated terms applicable to your order. Any Early Termination Payment depends on the termination ground and applicable Schedule.

### ***What happens to backup data when we leave?***

We must delete Customer Data from our environment at the end of the Service Period and the customer is solely responsible for taking a copy beforehand. The general terms do not set a grace period, so agree an exit data window and format before signing.

***What is Offsite Backup as a Service from you?***

Offsite Backup as a Service is our service that provides managed offsite backup, keeping an independent copy of critical data away from primary infrastructure to strengthen recovery and business continuity.

***What category and service type do you classify Offsite Backup as a Service under?***

We classify Offsite Backup as a Service under the category 'Cloud' with a service type of 'Cloud, backup and recovery'.

***Which geographic area does your Offsite Backup as a Service cover?***

The service is offered to customers in Australia, as it is listed with an area served of Australia.

***Who provides the Offsite Backup as a Service?***

The service is provided by us, an organization identified by its logo and branding on the page.

***How does Offsite Backup as a Service relate to your broader backup obligations?***

Where the applicable agreement includes backups, the v3.6 framework requires running backup software at agreed intervals and re-running reported failures after addressing the root cause. A restore returns the version of Customer Data that existed at the relevant backup. Read the backup duties across the Service Order, Service Description and Schedule together.

***Does offsite backup guarantee restoration of uncorrupted data?***

No. According to our backup service terms, backups restore data to the state it existed when backed up—including if that data was already corrupted or damaged at that time.

***Where is data backed up by you stored?***

Our general data-sovereignty statement describes Australian storage and processing. Confirm the locations of your backup data, replicas, metadata and support access in the proposed service; that general statement does not establish every deployment's configuration.

***How does offsite backup relate to other blueAPACHE managed services?***

Backup, cloud, disaster recovery and managed services are related capabilities. Confirm the included workloads, hosting, integrations and operating responsibilities in your order; their presence in the portfolio does not mean every service is included or uses the same platform.