

Disaster Recovery as a Service | blueAPACHE

Canonical: <https://www.blueapache.com/services/disaster-recovery-as-a-service>

Details:

Summary

Disaster Recovery as a Service is our managed recovery capability for organisations that need critical systems restored after a major outage or data-loss event. Its contractual name is emPOWER IT Continuity Services (DRaaS), Schedule 4 of our General Terms and Conditions v3.6, and the recovery platform, locations and connectivity should be confirmed for the proposed solution.

Key facts

Label	Value
Contract name	emPOWER IT Continuity Services (DRaaS), Schedule 4
Scope of obligation	Restoration of Customer Data and Software subject to the agreed Restore Time Objective and Recovery Point Objective in the Schedule (clause 3.17)
Recovery objectives	Confirm the agreed Restore Time Objective and Recovery Point Objective, covered workloads and measurement definitions in the applicable Schedule and Service Order
Delivery platform	Confirm the recovery platform and connectivity in the agreed architecture
Data location	Australian-based data centres, Australian legal jurisdiction
Certification scope	emPOWER IT Continuity Services (DRaaS) listed on ISO/IEC 27001:2022 certificate 202507-118
Data-loss liability	Clause 19.4(a) links exclusions and restoration-cost limits to the relevant backup/DR obligation and its breach; subject to clauses 19.1 and 19.2, applicable law and the complete agreement
Business continuity plan integration	Opt-in Action Plan under clause 15, chargeable as a Professional Service
APRA-related BCP provisions in v3.6	Where clause 10 applies and the customer requires a BCP under clause 15: joint testing every six months or on reasonable request, results within

	seven days; clause 10.5 allocates costs
Default contract term in v3.6	36 months except Professional Services, unless the Service Description or Service Order specifies otherwise

What is included

Contractually, clause 3.17 of the general terms states that where the Schedule expressly includes disaster recovery services, "the obligation to provide disaster recovery services is limited to the restoration of Customer Data and Software that is the subject of the agreed Restore Time Objective and Recovery Point Objective as set out in the relevant Schedule".

Clause 3.17 refers to the agreed Restore Time Objective and Recovery Point Objective in the relevant Schedule. Confirm their values, definitions, measurement start and end points, and covered workloads in the applicable agreement. General Terms v3.6 use "Restore Time Objective" without defining it in clause 1, so do not assume a particular recovery clock from the service name alone.

What is not included

Reconcile the current systems inventory with the agreed recovery scope and any signed variations. A system added later may be brought into scope through a variation; its recovery obligations cannot be determined from its installation date alone. 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.

Agree the DR testing cadence, invocation procedure and authority to declare a disaster in the service documents. General Terms v3.6 include a conditional APRA-related BCP testing regime in clause 10.4, rather than a universal DRaaS test schedule. Clause 15 allows the customer to request actions supporting its BCP; blueAPACHE will not unreasonably refuse. Creating, maintaining and activating the Action Plan is chargeable as a Professional Service under that clause. Check your proposal for any separately included planning work. Note that the defined term "Restore Time Objective" used in clause 3.17 is not itself defined in clause 1, which defines only "Recovery Point Objective"; buyers should confirm the intended term in their Schedule.

Who it is for

The service suits organisations whose core applications cannot tolerate an extended outage and who want a contracted recovery target rather than a best-efforts restore. Honan Insurance took emPOWER DRaaS alongside emPOWER Cloud, IaaS, Managed Services and WAN as part of a whole-of-business move, and our data sovereignty statement makes the service relevant to organisations with Australian residency obligations. Clause 10 of General Terms v3.6 is framed around APRA-regulated entities and material business activities under CPS 231. Where it applies and the customer requires a BCP under clause 15, clause 10.4 specifies minimum content and joint testing every six months or on reasonable request, with results within seven days. Confirm the applicable agreement and regulatory requirements rather than treating that historical clause reference as current regulatory guidance.

How it is delivered

Clause 8 of General Terms v3.6 describes Transition In Services immediately following the Service Commencement Date: due diligence, monitoring-platform configuration where applicable, support documentation and agreement on meetings and reporting. Confirm the specific onboarding deliverables and recovery objectives for each protected workload in your service documents.

Ongoing operation follows the backup obligation in clause 3.14: run backup software at the agreed intervals and, where the software reports a failure, address the root cause and re-run until success is recorded. A restore returns the version of Customer Data that existed at the time of the relevant backup, including if that data was already corrupted. Emergencies are handled under clause 3.13, with as much notice as practical and best efforts to restore Services as soon as possible; an Emergency interruption is a Reasonable Excuse that disapplies Service Levels for its duration.

Commercial model

DRaaS is contracted on a Service Order with a Schedule 4 attachment. Fixed fees are invoiced monthly in advance and any usage-based components monthly in arrears (clause 12.1), with direct debit as the default payment method and GST additional. No price list for DRaaS is published. Costs of Action Plan work under clause 15 and of BCP testing for APRA-regulated customers under clause 10.5 are charged at the Time and Materials Rates on the Service Order, or our then-current rates if none are stated.

Support and service levels

Customers who also hold emPOWER Managed Services receive its unlimited 24/7 help desk, staffed in Australia during business hours and by a global team after hours. Business Hours in the general terms are 0700 to 1900 AEST/AEDT on Business Days.

The recovery Service Levels are the RTO and RPO in the Schedule. We must meet or exceed them except to the extent a Reasonable Excuse contributes to the failure (clause 3.7), which includes customer-side faults, third-party software used by us, and Emergencies. Measurement is by our tools and the results are final and binding (clause 3.8). The general terms contain no service credit regime; any remedy for a missed recovery objective is set in the Schedule. Monthly reports on Service Level performance are due within five Business Days of month end.

Related services

Offsite Backup as a Service provides the independent data copy that recovery depends on; Private and Public SaaS Backup covers Microsoft 365 and other SaaS data that DRaaS for infrastructure does not reach; Storage as a Service provides immutable S3-compatible storage for long-retention data. emPOWER Cloud is the platform, and emPOWER Core Network and Data Centre Interconnect is the path between production sites and the recovery environment. emPOWER Backup for Microsoft Entra ID protects identity data on the same private cloud.

Buying questions

Contract term and renewal. The default Minimum Service Period is 36 months from the Service Commencement Date (clause 2.6). 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. The customer may terminate for unremedied breach after 20 Business Days' notice, or on blueAPACHE ceasing business or becoming insolvent (clause 24.1). We may terminate or suspend 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 and unpaid minimum commitments depend on the termination ground, the applicable Schedule and the complete agreement. Confirm the clause 25.2 consequences for the proposed exit.

What to fix on the Service Order. The RTO and RPO for every protected workload; the testing cadence and who may invoke recovery; whether an Action Plan under clause 15 is required and at what rates; the exit data window and format, because clause 9.1 requires us to delete Customer Data at the end of the Service Period and makes the customer solely responsible for taking a copy first; and, for APRA-regulated customers, the clause 10.4 BCP content.

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. 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. The loss-of-profit, revenue and interruption exclusions must also be read with those qualifications.

Agreeing what counts as successful recovery

Identify protected applications and data, their dependencies, recovery order and who declares a disaster. Specify how recovered workloads are checked and normal operations resume. A backup copy, a running virtual machine and a usable business application are different milestones; the agreement should make the required endpoint clear. Obtain the recovery objectives, measurement definitions and testing commitments for the proposed service.

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.

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.

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.

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.

Related

Cloud pillar hub

emPOWER Cloud

Offsite Backup as a Service

Private and Public SaaS Backup

Storage as a Service (Private S3)

emPOWER Core Network and Data Centre Interconnect

Managed Services pillar hub

Case study: Honan Insurance

Case study: Brotherhood of St. Laurence

Industry: Financial services

Industry: Healthcare and aged care

Service Agreement terms

Support

Contact blueAPACHE

What is the contractual name of your DRaaS?

emPOWER IT Continuity Services (DRaaS). It is Schedule 4 of the General Terms and Conditions v3.6 and one of the ten services listed in scope on our ISO/IEC 27001:2022 certificate.

What does the service actually restore?

Clause 3.17 of General Terms v3.6 limits the DR obligation to Customer Data and Software subject to the agreed Restore Time Objective and Recovery Point Objective in the relevant Schedule. Check the complete agreement and variations for the current protected scope.

What RTO and RPO do you offer?

Confirm the objectives for each protected workload in the applicable agreement. Clause 3.17 refers to agreed objectives in the relevant Schedule; the Service Order and any variations may also define or change the commitment.

How much data could I lose in a recovery?

Up to the agreed Recovery Point Objective. A restore returns the version of data that existed at the last successful backup, and clause 3.14 makes clear that if that data was already corrupted, the same corrupted data is what gets restored.

Is recovery tested?

Where clause 10 of General Terms v3.6 applies and the customer requires a BCP under clause 15, clause 10.4 provides for joint BCP testing every six months or on reasonable request and results within seven days. Clause 10.5 allocates the costs. Confirm the DR test scope and schedule for your order.

Where is the recovery environment located?

On emPOWER Cloud in Australian-based data centres, subject to Australian legal jurisdiction, according to our data sovereignty statement. The statement does not name the specific facilities.

What are you liable for if recovery fails?

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.

Does DRaaS include a business continuity plan?

Check the planning deliverables in your DRaaS proposal. Clause 15 of General Terms v3.6 separately allows a customer to request an Action Plan supporting its BCP; blueAPACHE will not unreasonably refuse. That clause makes creation, maintenance, updates and activation work chargeable as a Professional Service.

Can we take the service down for maintenance?

Scheduled maintenance runs within the windows in the Schedule or on at least three Business Days' notice otherwise. In an Emergency, we give as much notice as practical, the Service may be

unavailable, and the interruption counts as a Reasonable Excuse.

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 applicable termination ground and Schedule.

What happens to my data at the end of the contract?

We delete Customer Data from our environment at no cost as part of disengagement, and the customer must take their own copy before expiry or termination. Negotiate an explicit exit data window on the Service Order, because the general terms do not state one.

What is Disaster Recovery as a Service (DRaaS) offered by you?

Disaster Recovery as a Service is a managed recovery capability for restoring protected Customer Data and Software. General Terms v3.6 refer to emPOWER IT Continuity Services (DRaaS) under Schedule 4. Confirm the recovery platform, locations, connectivity and workload scope in your proposal and agreement.

What is the scope of your obligation when a Service Agreement includes DRaaS?

According to Clause 3.17 of the General Terms and Conditions, our obligation to provide disaster recovery services is limited to the restoration of Customer Data and Software that is the subject of the agreed Restore Time Objective and Recovery Point Objective as set out in the relevant Schedule.

What is a Recovery Point Objective (RPO) in the context of your DRaaS?

The Recovery Point Objective specifies the maximum period within which Customer Data might be lost. It represents the latest point in time to which Customer Data must be restored following a disaster, effectively establishing the maximum acceptable amount of data loss measured in time from the latest backup.

What is a Restore Time Objective (RTO) in your DRaaS?

General Terms v3.6 use the term Restore Time Objective in clause 3.17 without defining it in clause 1. Confirm the agreed objective, measurement start and end points and recovery endpoint in the applicable Schedule and Service Order.

How are RPO and RTO targets determined for individual customers?

Clause 3.17 of General Terms v3.6 refers to agreed Restore Time and Recovery Point Objectives in the relevant Schedule. Confirm the values and covered workloads in the applicable agreement, including the Service Order and any variations.

What does the restoration under your DRaaS actually include?

Disaster recovery services restore Customer Data to the agreed Recovery Point Objective and Software subject to the service to the agreed Restore Time Objective. The restoration delivers only the version of data and software as governed by these agreed objectives.

Under which category and service type do you classify Disaster Recovery as a Service?

We classify Disaster Recovery as a Service under the category 'Cloud' with the service type 'Cloud, backup and recovery,' and the service area served is Australia.