SERVICE SCHEDULE

PULSANT DISASTER RECOVERY AS A SERVICE

This is a Service Schedule as defined in the Conditions. Where the Services set out in this Service Schedule form part of the Services to be supplied under a Contract (as defined in the Conditions), this Service Schedule forms part of the Contract.

In this Service Schedule, references to Clauses are to Clauses of the Conditions, and references to paragraphs are to the paragraphs of (i) this Service Schedule or (ii) whichever other document is specifically referred to.

1 Additional Definitions

In this Service Schedule the following words and expressions shall have the following meanings:

1.1 **"Cloud Hosts"** – the physical host servers, fully managed by the Supplier, which are connected to either enterprise shared storage or connected via the Supplier's IP network to shared storage, and/or the internet to provision the relevant Pulsant Cloud Service.

1.2 **"Conditions" –** the Pulsant General Terms and Conditions which is displayed on the Pulsant website.

1.3 **"Service Description Document"** – the document which sets out the scope and description of the Services being provided by the Supplier.

1.4 **"DRaaS"** – Disaster Recovery as a Service provided through the use of software for the replication of Virtual Machines between cloud infrastructures.

1.5 **"Failback Test"** –A Failback Test is a sequence of two full failover actions. The first performs a full failover of the environment to the Recovery Site. Whilst service is provided from the Recovery Site testing should be carried out by the Customer to validate successful failover of their services. The second failover returns services to the Primary Site where once again the customer should test and validate that all services are successfully restored. This process is always intrusive to the Primary Site services and will involve a short period of service downtime during the process. This process shares all risks associated with a full, live failover event but is the truest test of a Disaster Recovery strategy.

1.6 **"Failover Test"** – A process which performs the failover action to the Recovery Site but without removing the Primary Site from service. The customer can perform full testing of the Disaster Recovery environment in the Recovery Site to validate success of Disaster Recovery without affecting services in the Primary Site. At the Virtual Machine level this process is non-intrusive to the Primary Site services.

1.7 **"Hypervisor"** – the software and service layer provided by the Supplier to deliver one or more Virtual Machines on either a single Cloud Host or a resilient Cloud Host in order to deliver a secure virtual hosting platform;

1.8 **"Primary Site"** – The normal location or environment in which services run.

1.9 **"Recovery Site"** – The location or environment to which services are restored and temporarily run whilst in their Disaster Recovery position.

1.10 **"RPO"** – The RPO specifies the maximum time lag between data stored on the primary and disaster recovery locations – the maximum window in which data may be lost during a total loss of the primary location. Data replication cannot be immediate between distinct sites as it would then become a single point of failure. Therefore, there is an inherent time lag between the primary and disaster recovery locations.

1.11 **"RTO" –** Recovery Time Objective, the elapsed time for the Disaster Recovery failover action, which restores Virtual Machine(s) to the Disaster Recovery destination, to complete once initiated. The Supplier defines the service as being restored when virtual servers are powered on in the Disaster Recovery environment. The RTO does not include any time required to perform a graceful shut down of any non-failed workloads prior to the failover action starting.

1.12 **"Pulsant Cloud"** – Pulsant Enterprise Cloud or Pulsant Private Cloud, as specified in the Order Form.

1.13 **"Virtual Data Centre (vDC)"** – the capacity of Ghz or vCPUs, RAM and storage allocated to the Customer which can be assigned to Virtual Machine(s);

1.14 **"Virtual Machine(s)"** – an operating system with a pre-determined quantity of memory, CPU processing capacity and storage that resides on a Hypervisor and the shared hardware and network infrastructure that forms the Pulsant Cloud.

2 DRaaS – Service Scope and Description

2.1 DRaaS is a software enabled replication technology that allows Virtual Machines running on the Primary Cloud Host to be restarted on a secondary, remote Pulsant Cloud Platform in the event that the primary platform becomes unusable.

2.2 The scope of the Services being provided by the Supplier is detailed in the Service Description Document which also contains recommended specific considerations under the section “Service Dependencies and/or Related Services”. The Customer confirms that it has considered and retains full responsibility for all scenarios relating to failure conditions and functionality of each related or dependent service and that the Supplier has no responsibility for any failure of any of these related or dependent services.

2.3 In the event of a disaster, the Customer may invoke a disaster recovery event at which point the Supplier will invoke the replicated copy of each Virtual Machine on the Pulsant Cloud platform.

2.4 Where the Customer purchases the reserved DRaaS solution, the total required resources are ring-fenced and reserved for the Customer’s exclusive use, and the Supplier provides full assurance that the resources will be 100% available to the Customer.

2.5 Where the Customer purchases the standard, non-reserved DRaaS solution, the resources are drawn from the Pulsant Cloud general pool and will be allocated to the Customer on a first come first served basis. Accordingly the Customer accepts that there may be circumstances where the full resources needed are not available, for example where a large number of Virtual Machines (for a single large Customer, or multiple Customers) experience a disaster recovery event at the same time. The Customer accepts full responsibility and liability where resources are non-reserved.

2.6 In the event that replication of Virtual Machines is from a compatible Customer managed cloud platform to the Pulsant Cloud, the Supplier is unable to manage performance in accordance with the Service Levels in Clause 4, as these configurations rely on an infrastructure that is not managed by the Supplier. The Customer will be responsible for ensuring network compatibility, and secure connectivity between the Customer cloud platform and the Pulsant Cloud platform. In the event that changes or other service elements are required to bring the service live, over and above the booting of the VM, the customer will retain responsibility for this activity.

2.7 The Customer accepts that it should have a suitable back up system in place to protect their environment and data separate from this solution. The replication technology used will not protect from virus infection, or other types of data corruption nor loss that occurs on the source cloud environment. In the event that the source cloud platform has been corrupted, there is a risk that any standby Virtual Machines may not be operational post replication, and the Supplier would not be liable for any failure to satisfy the Service Levels in paragraph 4.

2.8 The Customer is responsible for ensuring that any software licensing not provided by the Supplier is appropriate for use, where the licensed software transitions between the production source and target location.

2.9 In the event that a suspected hardware or software issue is identified, the Supplier will only provide end to end diagnostics if the connectivity, hardware and software is part of the Supplier managed solution.

3 Disaster Recovery Testing

3.1 The Customer acknowledges that it is best practice to perform disaster recovery tests to prove that service can be restored following a disaster recovery event.

3.2 The Customer is entitled to perform either;

3.2.1 two Failover Tests in any 12 month rolling period, or

3.2.2 one Failback Test in any 12 month rolling period,

both such periods starting from the Service Commencement Date.

3.3 The Customer acknowledges that the Failback Test (which for the avoidance of doubt comprises a scheduled full failover event and subsequent failback) will affect the production environment.

3.4 The Customer must give the Supplier no less than 30 days prior written notice of any planned disaster recovery test.

3.5 Any Service Levels assigned to the original service shall not be applicable during any planned disaster recovery test.

3.6 Assessment of the outcome of any Disaster Recovery testing remains the responsibility of the Customer. If the Virtual Machines transfer successfully (or boot in the case of a Failover Test) and the data is synchronised within the limits of the RPO, Pulsant will consider the test a success.

3.7 In the event that the Virtual Machines do not successfully start or data has not synchronised correctly (if applicable – see clause 2.6), this test will not be considered to count towards the annual test limit.

4 Service Levels

4.1 The Supplier will use its reasonable endeavours to deliver the following Recovery Times in respect of disaster recovery events as set out in the table below.

4.2 Disaster recovery failover actions must always be triggered by telephone from a primary account contact or a specifically authorised contact.

4.3 Where the failed site is a Supplier managed environment, this call may be triggered by the Supplier following an initial assessment of the impact of the failure and the time to fix. In the event that the Supplier deems it necessary to invoke this option, it may be undertaken without prior notification of the client.

4.4 It is agreed between the parties that there may be a delay to certain software services operating following a system boot and the SLAs will not be enforceable for the duration of time when there is no network connectivity at the disaster recovery site.

SLA DATA	Service Hours	Recovery Time	Fee Credits
RTO	24/7/365	30 minutes	Pro rata proportion of the Monthly Charges for any Period of breach
RPO	24/7/365	10 minutes	Pro rata proportion of the Monthly Charges for any Period of breach
Maximum Time in Disaster Recovery	N/A	30 days in any 12 month period (including testing) Where Disaster Recovery resources are reserved no limit applies.	N/A

Event Type	Service Hours	Response Time
Critical	24/7/365 (Issue must be notified by telephone)	Within 15 minutes
Impacting Service	24/7/365 (Issue must be notified by telephone)	Within 30 minutes
Routine	Business Hours	Within 30 minutes measured during Business Hours

5 Fee Credits

5.1 Any Fee Credits which fall due pursuant to clause 4 above are payable subject to and in accordance with Clause 5 of the Conditions.

6 Planned maintenance

6.1 Save in situation which is an Event of Force Majeure or in the case of an emergency, where the Supplier considers (in its sole discretion) that it is necessary to carry out maintenance activities that will affect or can reasonably be expected to affect the Customer's operations, the Supplier shall notify the Customer at least 48 hours in advance of the commencement of the works detailing the nature of the work to be carried out and the timetable for completion of the works. These works will be carried out in accordance with the Supplier's standard procedures which are available upon request by the Customer. In the case of an Event of Force Majeure or an emergency, no advance notice is required.

6.2 During the period of Planned Maintenance, the SLA for RTO and RPO will not apply.