SERVICE SCHEDULE

PRIVATE CLOUD

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   **"Guest"** – a Virtual Machine and Operating System which runs on a Host server.

1.2   **"Host"** – a physical server running a Hypervisor which runs and manages Guest Virtual Machines.

1.3   **"Hypervisor"** – a server Operating System designed to run on a physical server (the Host) which provides the ability to securely run one or more Virtual Machines (the Guests). The Hypervisor ensures that each Virtual Machine is entirely segregated from every other, and manages the resources which are available to each.

1.4   **"Compute resources"** – CPU and memory which will be allocated to Virtual Machine(s).

1.5   **"Operating System"** – a software system designed to run directly on physical or virtual hardware which manages the hardware state and allows running of additional application software.

1.6   **"Private Cloud"** – a specific configuration of hardware and software components that provides a virtualisation environment that is dedicated to the Customer. Specifically, the Supplier defines "Private Cloud" as a private virtualisation environment where the Customer has a private instance of the system controller (and therefore the environment configuration) and dedicated, physical cloud Hosts. Some components of the platform may be either physically dedicated or logically dedicated as specified by the Service Order Form.

1.7   **"Virtual Machine", "VM"** – a virtualised server environment running a Guest Operating System, including the data files which define the Virtual Machine and those which contain the Virtual Machine's associated virtual disk drives and their data.

2   Private Cloud - Service Scope and Description

2.1   Pulsant Private Cloud delivers a platform which gives the Customer access to virtualisation resources in which the Customer can operate Virtual Machines.

2.2   Private Cloud Services are provided to the Customer for so long as the Contract remains in force in accordance with the terms of this Contract and the Supplier's acceptable use, security and access policies and procedures.

2.3   Private Cloud Services are subject to payment by the Customer of the Supplier's Charges for installation and support Services, as set out in the Order Form or as subsequently agreed between the parties from time to time.

2.4   The Supplier will provide the Customer with the following:

2.4.1   Compute resources which are provided by physical servers which are for the sole use of the Customer, and for the allocation to Virtual Machines which are created by the Customer or the Supplier. The specification of the physical servers is detailed on the Service Order Form.

2.4.2   Management services which control and assure the availability of the resources in line with the SLA as defined in paragraph 4.2 of this Service Schedule. Management services include:

2.4.2.1   Installation and configuration of the Hypervisor software required to create and run Virtual Machines in the Private Cloud.

2.4.2.2   Monitoring of the availability and performance of the Hypervisor and remediation of issues, notifying the Customer where appropriate.

2.4.2.3   Application of Hypervisor patches as recommended by the vendor, subject to the Supplier's testing and approval.

2.4.2.4 Re-installation of the Hypervisor following a failure of an underlying physical or virtual server.

2.4.2.5 Support for virtual servers that fail to start to boot, where those servers' Operating Systems are managed by the Supplier.

2.4.2.6 Management of resource reservations and prioritisation of virtual hardware.

2.4.2.7 Management of logical storage volumes and capacity utilisation.

2.4.2.8 Management of resiliency configuration including ensuring that capacity deployed remains within the constraints of specified resiliency policies.

2.4.2.9 Monitoring and management of the availability of the platform.

2.4.2.10 Management of the physical network.

2.4.2.11 Configuration of virtual networks through the physical network.

2.4.3 Storage resources, which are provided as storage volumes for allocation to Customer Virtual Machines. These resources are for the sole use of the Customer. Storage resources are provided as specified on the Service Order Form by either:

2.4.3.1 A Customer dedicated storage system, subject to the separate service schedule for Managed Storage System.

2.4.3.2 Storage resources provided by the Supplier's Cloud Storage service, subject to the separate service schedule for Cloud Storage.

2.4.4 Storage network(s), over which the storage resources are provided, are logically secured. These networks are provided as specified on the Service Order Form by either:

2.4.4.1 Customer dedicated network switching, subject to the separate service schedule for Managed Switch.

2.4.4.2 The Supplier's Cloud Fabric service, subject to the separate service schedule for Cloud Fabric.

2.4.5 Management network(s), which enable control of the assigned Virtual Machine resources from the virtualisation management services and systems, are logically secured and for the sole use of the Customer. These networks are provided as specified on the Service Order Form by either:

2.4.5.1 Customer dedicated network switching, subject to the separate service schedule for Managed Switch.

2.4.5.2 The Supplier's Cloud Fabric service, subject to the separate service schedule for Cloud Fabric.

2.4.6 Virtual Machine networks, to which the Customer's Virtual Machines connect, are logically separated and for the sole use of the Customer. These networks are provided as specified on the Service Order Form by either:

2.4.6.1 Customer dedicated network switching, subject to the separate service schedule for Managed Switch.

2.4.6.2 The Supplier's Cloud Fabric service, subject to the separate service schedule for Cloud Fabric.

2.4.7 Network perimeter security, which provides protection of the trusted Private Cloud networks from external, untrusted networks, is provided by the Supplier's Managed Firewall service. The firewall appliances are dedicated to the Customer, and are for the sole use of the Customer, running either as virtual appliances on the Customer's Private Cloud environment or as physical appliances. Firewalls are provided subject to the separate service schedule for Managed Firewall Services.

2.4.8 Basic installation of an Operating System on each Virtual Machine and configuration to the minimum required for remote administrative access.

2.4.8.1 Any installed Operating System versions will be shown on the Order Form, and will be restricted to those Operating System versions supported by the Supplier, as advised at point of sale.

2.4.8.2 Management of Virtual Machine Operating Systems is not included in the Service. Such management, if required, must be purchased as the separate Managed Server service and would be subject to the separate service schedule for Managed Server.

2.4.8.3 The Supplier will not provide any support of Virtual Machines running Operating Systems not managed by the Supplier.

2.5 Private Cloud must be specified and maintained so as ensure it meets the requirements placed on it such as performance, capacity and security. The Customer holds full responsibility for ensuring that its requirements are met and for informing the Supplier where those requirements change so the Supplier may recommend changes to the Private Cloud to accommodate.

2.6 Private Cloud is provided to the Customer on a managed basis where the Customer is not able to directly configure the Private Cloud platform. Changes to the configuration of the platform may requested by the Customer. Change requests received by the Supplier are reviewed prior to implementation so as to confirm they are appropriate to achieve the Customer's objective and that they uphold performance, capacity and security practises and deployment standards within the Service.

2.7 The Customer confirms that it has considered and accepts full responsibility for all scenarios relating to any failure conditions and functionality of each related or dependent service where those services are not provided by the Supplier.

2.8 The Customer accepts that Private Cloud environments have various high availability features allowing for continuation of normal service in the event of failure of physical components. Each feature recovers from a component failure in a particular way and some involve a short period of consideration of the failure scenario and then a reaction to recover if required. During this consideration and reaction period, some interruption of services may occur and during this time the Private Cloud is considered to be available as it is operating within its designed parameters. All Private Cloud high availability features and recovery processes are entirely automated by the Private Cloud virtualisation management services and systems.

2.9 The Supplier will configure the virtual environment and virtual hardware resident on the environment within the best practices set out by the Hypervisor vendor. Where the Customer requests changes which breach best practices the Supplier shall advise against proceeding, and should those changes become applied against Supplier's advice the Supplier is no longer able to guarantee service levels.

2.10 The Supplier will monitor the infrastructure which forms the Private Cloud in line with those component services (such as Pulsant Dedicated Server) and will resolve any issues with consideration of how the Private Cloud environment operates. For example, Private Cloud physical Host servers will be specified with a minimum of N+1 and where that level is maintained a physical server can be safely removed from the Private Cloud for maintenance rather than risking running Virtual Machines with live changes.

2.11 The Supplier will monitor the available capacity and performance of the Private Cloud platform and make recommendations for capacity increments as required. Where recommendations are made by the Supplier and not accepted by the Customer, the Supplier will not guarantee the availability of the Private Cloud.

2.12 The Customer is responsible for ensuring that a suitable data backup service is maintained to protect data within the Private Cloud. Where the Supplier provides such backup services the Customer remains responsible for determining which data must be protected and communicating that requirement to the Supplier.

2.13 Major version upgrades of the Hypervisor will not be performed as a standard part of this Service, and would be considered additional chargeable work if requested by the Customer.

2.14 The Supplier will not provide any training or education on how to operate the Private Cloud.

2.15 Following expiry or Termination of the Contract:

2.15.1 The Supplier will delete all virtual disks and Virtual Machine instances created within the Service, which will result in loss of all Customer data stored by the Service.

2.15.2 Where data storage is provided from shared resources on a multi-tenanted platform, the Supplier has no obligation to physically or logically destroy the storage media beyond the logical deletion of Virtual Machines and disks, and may reallocate the storage media to other customers.

2.15.3 The Customer accepts that the nature of shared storage means that the physical storage media of any deleted data may be re-allocated to different customers and overwritten multiple times by new data, making data recovery from this media practically impossible.

2.15.4 Where data storage is provided by physical servers or disks which are for the sole use of the Customer, the Supplier will perform a logical erasure of all Customer data. If agreed with the Customer, the Supplier will oversee the physical destruction of the storage media by a trusted third-party organisation, noting that this activity may incur additional charge. A certificate of secure destruction will be provided in this case.

2.15.5 It is the Customer's responsibility to ensure that any required data is transitioned to an alternative provider prior to deletion or destruction, in accordance with Clause 15 of the Conditions.

3 Private Cloud Security

3.1 Private Cloud and its component infrastructure services implement technology designed to ensure security is maintained where configured within the environment. Where Private Cloud is configured to enforce internal security (for example, network separation between groups of Virtual Machines) those configurations will be mirrored by the Supplier in any infrastructure services that participate in the configuration. Where changes are requested that could compromise security principles the Supplier will advise and recommend available alternatives.

3.2 Where untrusted networks, such as the Internet, are connected to the Private Cloud, the Supplier recommends in all cases that a fully capable firewall is employed as a perimeter security measure. Where such recommendations are not employed, the Supplier reserves the right to either suspend the SLA or in cases where a potential threat to the Customer environment or a Supplier environment is identified suspend and prevent access to the Services from the internet and/or the Pulsant Private Cloud network(s).

4 Service Levels

4.1 The Supplier will use its reasonable endeavours to deliver the following Response Times in respect of incidents as set out in the table below.

Event Priority	Definition	Service Hours	Response Time
P1	• Total loss of production service; or • A significant revenue, operational, or safety impact on the entire company; or • Service degraded, affecting the entire company	24/7/365	Within 15 minutes
P2	• Partial loss of service affecting the company; or • Service degraded, affecting multiple departments or a single site; or • There is the potential of significant revenue, operational, or safety impact to the company if not resolved quickly	24/7/365	Within 30 minutes
P3	• Service degraded, affecting non-production services; or • Loss of service affecting a single user	Business Hours	Within 1 Hour
P4	• Degraded service affecting a single user	Business Hours	Within 2 Hours
P5	• Request for information	Business Hours	Within 4 Hours

4.2 The Supplier will use its reasonable endeavours to deliver the following Service Levels in respect of the Services as set out in the table below.

4.2.1 The below table defines the SLA for the Private Cloud service.

4.2.2 Consumption of Private Cloud Services relies on connectivity to the Services. This SLA defines the provision of the Private Cloud Service only and does not include such connectivity.

Pulsant

Measure	Description	Value	Fee Credits
Service Hours	The hours during which the service and SLA is provided	24/7/365	
Availability: single-site Private Cloud	% of the service hours during which service availability is guaranteed (excluding Planned Maintenance)	99.995%	Pro rata proportion of the Monthly Charges for any Non-Availability Period
Availability: dual-site deployment with DRaaS	% of the service hours during which service availability is guaranteed (excluding Planned Maintenance)	99.999%	Pro rata proportion of the Monthly Charges for any Non-Availability Period

4.3   Fee Credits

4.3.1   Any Fee Credits which fall due pursuant to this paragraph 4.3 are payable subject to and in accordance with Clause 5 of the Conditions.

4.3.2   A pro rata proportion shall be calculated according to the number of complete minutes in the relevant calendar month and the number of complete minutes of Non-Availability in that calendar month.

4.3.3   "Monthly Charge" means the recurring Charges for the relevant Component for the relevant calendar month, net of VAT.

4.3.4   "Availability" means the percentage of the Service hours during which Service availability is guaranteed, not including Planned Maintenance.

4.3.5   "Non-Availability" means a period of time during which the relevant Service is unavailable in breach of the Availability Service Levels set out in paragraph 4.2 above.