SERVICE SCHEDULE

PULSANT CLOUD BACKUP

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 **"Account Encryption Key"** — a key used by all DS-Clients connecting to a single Customer account.

1.2 **"Cloud Backup"** — a capacity-based storage solution onto which the Customer can write compressed, de-duplicated, encrypted backup data via DS-Client.

1.3 **"Conditions"** — the Pulsant General Terms and Conditions which are displayed on the Pulsant website.

1.4 **"DS-Client encryption key"** — a key used by a specific DS-Client installation unique to the DS-Client on which it was created.

1.5 **"DS-Client"** — a component of Asigra's Cloud Backup and recovery software which provides end-to-end backup data recovery and protection and is installed on the Customer's LAN.

1.6 **"Pulsant Service Description – Cloud Backup"** — the document which sets out the scope and description of the Services being provided by the Supplier.

2 Cloud Backup — Service Scope and Description

2.1 Pulsant Cloud Backup provides an all-on-disk, cloud hosted storage vault and backup toolset designed to be simply installed and configured in a customer environment that will enable enterprise quality server backup protection and high speed data recovery.

2.2 Cloud Backup 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 Cloud Backup Services are subject to payment by the Customer of the Supplier's Charges for installation and support Services, where appropriate, calculated at its rates as set out in the Order Form or as subsequently agreed between the parties from time to time.

2.4 Cloud Backup can be provided to the Customer on a managed basis or a standalone capacity only basis.

2.5 The scope of the Services being provided by the Supplier is detailed in the Pulsant Service Description – Cloud Backup in the section headlined Management Scope. This Document 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 Cloud Backup 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. The Customer is responsible for ensuring all of its data is included within the scope of the Services and accordingly the Supplier will not be liable for any situation relating to any data where the Customer has excluded such data from the scope of the Services.

2.6 The Customer accepts that there are risks inherent in internet connectivity and the Supplier does not warrant the performance or impact on Services of any internet connectivity issues where such bandwidth is not wholly provided by the Supplier. The Supplier does not accept any responsibility for the impact the Services will have on the performance of the originating host or the bandwidth consumed by it.

2.7 The Supplier will only warrant the backup of applications and file structures where these are fully compatible with the relevant DS-Client statements.

3 Security

3.1 DS-Client encrypts all Customer data once read within the protected solution WAN.

3.2 There are two security keys that relate to Customer data security, namely the Account encryption key and the DS-Client encryption key. During installation of DS-Client the Customer can elect control options via “Enable Encryption Key Management”.

3.3 The Customer agrees and accepts that if it elects the option “Encryption Key Management Off” that the keys are not forwarded to the Supplier and the responsibility of safely storing the keys rests solely with the Customer. The Customer further accepts that if the keys become lost then it is impossible to restore the backup data and the Supplier will be unable to assist in any way. The Supplier will not be liable for any loss suffered by the Customer in relation to any misuse or loss of the encryption key.

3.4 On Termination, all data held by the Supplier, including secure encryption keys, will be removed and deleted by the Supplier and the Supplier will not hold a copy of this data or recover any data after such date of Termination. The Customer should therefore ensure that it has taken copies of all relevant data before the Termination date and shall remove any licensed software provided as part of the Services and return to the Supplier any onsite appliances provided by Pulsant within 14 days following the Termination date.

3.5 If the Customer wishes to reduce the volume of Cloud Backup data, it is recommended that the Customer undertake a full back up of data after such reduction in volume.

3.6 In accordance with Clause 12 of the Conditions, the Supplier does not accept any liability for any loss of data, corruption of data and any associated costs of replacement data.

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 Type	Service Hours	Response Time
Critical	24/7/365	Within 15 minutes
Service Affecting	24/7/365	Within 30 minutes
Routine	Business Hours	Within 30 minutes, measured during Business 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 Pulsant Cloud Backup Online Storage Vault component of the service, that is, the online storage platforms Pulsant hosts which receive backup data from customer environments via the DS-Client application.

4.2.2 Where DS-Client installations and protected environments are also managed by Pulsant, the SLAs for those managed services apply and include the Cloud Backup components within those environments.

Measure	Description	Value
Service Hours	The hours during which the service and SLA is provided	24/7/365
Availability	% of the service hours during which service availability is guaranteed (excluding planned maintenance in paragraph 6 below)	99.90%

4.3 Where incidents are identified within the provision of the Cloud Backup service, the Supplier shall not be liable for fixing these incidents where the Cloud Backup service is on a standalone capacity only basis, and in this instance the fix solutions and diagnostics can be made available to the Customer at the Supplier’s current professional services rates.

4.4 Where consumed Cloud Backup capacity exceeds the committed backup quota purchased by the Customer, the Supplier reserves the right to charge any excess at a unit price which is calculated as 1.25 times the average of the unit price across all live Cloud Backup contracts for that Customer. This is done in order to maintain the integrity of subsequent backups.

5 Fee Credits

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

	Service Hours	Target Availability	Fee Credits
Cloud Backup	24/7/365	99.90%	Pro rata proportion of the Monthly Charges for any Non-Availability Period

5.2 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.

5.3 "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.

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 SLAs will not apply.