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 **"Asigra"** — a third-party supplier of backup systems which the Supplier uses to provide its Cloud Backup Service.

1.2 **"Cloud Backup"** — a Service which provides storage capacity in the Supplier's data centre and allows the Customer to securely back up their data to the storage under either a Managed or Unmanaged consumption model.

1.3 **"DS-Client"** — a component of Asigra's backup solution which is installed in the Customer's infrastructure to manage backup jobs and provide end-to-end backup data recovery and protection.

1.4 **"Encryption Key"** — a software code unique to the Customer's backup Service, used to securely encrypt backup data during transmission and while at rest in the Cloud Backup storage vault, and to decrypt restored data.

1.5 **"Managed Backup"** — A Service option in which the Supplier provides full configuration and day-to-day operation of the Customer's backup jobs as well as providing and managing the DS-Client software and storage platform.

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

1.7 **"Unmanaged Backup"** — A Service option in which the Supplier provides and manages the storage platform and DS-Client software only and the Customer has responsibility for the configuration and day-to-day operation of its backup jobs.

2 Cloud Backup — Service Scope and Description

2.1 Pulsant Cloud Backup Service (as described in the "Pulsant Service Description – Cloud Backup" document) provides a cloud hosted storage vault and backup toolset, designed to be simply installed and configured in a customer environment, that will enable server backup protection and high speed data recovery.

2.2 The management scope of the Services being provided by the Supplier is illustrated in the "Pulsant Service Description – Cloud Backup" document, which also contains recommended specific considerations under the section "Service Dependencies and/or Related Services". 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.

2.3 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.

2.4 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.

2.5 The Customer's storage quota will be set out in the Order Form and the Customer will be charged on the basis of the maximum storage quota reserved whether that quota is fully used or not in any particular accounting period.

2.6 Where the Customer's consumed storage exceeds the Customer's contracted quota, 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.

2.7 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 connectivity 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.

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

2.9 Cloud Backup can be provided to the Customer on a Managed Backup basis or a Unmanaged Backup basis, as will be noted on the Order Form. The scope of these options will be as described in paragraphs 3 and 4 of this Schedule.

2.9.1 The entire Service will be provided as either Managed Backup or Unmanaged Backup; the Customer cannot mix these two Service options within a single Service Contract.

2.10 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.

2.11 The Supplier will only warrant the backup of applications and file structures where these are fully compatible with the Asigra software or as advised by the Supplier, noting that such compatibility may be revised from time to time by Asigra.

2.12 The Customer must provide, or authorise the Supplier to provide, sufficient server resources, either virtual or physical, to run the required DS-Clients.

2.13 Management of the DS-Client and the server on which it runs is the sole responsibility of the Supplier and Customer will not be permitted administrative access to this server.

2.14 Following expiry or Termination of the Contract:

2.14.1 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.

2.14.2 It is the Customer's responsibility to ensure that any required data is transitioned to an alternative provider prior to deletion, in accordance with the Conditions.

2.14.3 The Customer shall remove any licensed software provided as part of the Services and return to the Supplier any on-site appliances provided by the Supplier within 14 days following the Termination date.

2.14.4 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.

2.14.5 The Supplier has no obligation to physically or logically destroy shared data storage beyond the logical deletion of virtual machines and disks, and may reallocate the storage media to other customers.

2.14.6 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.

2.14.7 The Supplier will delete all instances of the DS-Client software, including all associated data and configuration information, from the Customer's infrastructure.

2.15 The Customer's backed-up data will be stored within a data centre operated by the Supplier.

2.15.1 Where there is a choice of possible backup storage locations, the choice will be made by the Supplier.

2.15.2 The Supplier will ensure that the chosen backup location is not the same data centre that holds the Customer infrastructure that is being backed up.

2.15.3 All backed-up data will remain on-shore in the UK.

3 Managed Backup

3.1 Where the Order Form shows "Managed Backup", the Supplier will:

3.1.1 Provide a secure storage vault of the contracted capacity within a data centre managed by the Supplier.

3.1.2 Deploy one or more DS-Clients into the Customer infrastructure.

3.1.3 Manage the DS-Client and the server on which it runs.

3.1.4 Create configure, and test backup sets and backup policies.

3.1.5 Monitor backup jobs for success or failure and inform the Customer of any failed backup job.

3.1.5.1 A failed backup jobs is treated as a P3 incident for SLA purposes, as defined in paragraph 6.1.

3.1.6 Re-configure backup sets and policies as directed by the Customer throughout the lifetime of the Contract.

3.1.6.1 Where the Customer has identified a need for a backup policy change, for example to reduce storage needs, but is unable to define what specific policy changes are needed, the Supplier can advise on how best to achieve the desired outcome; this would be chargeable consultancy work.

3.1.7 Restore backups on request.

3.1.8 Store a secure copy of the Encryption Keys.

3.1.9 Perform a maximum of four (4) test restores of data per year, on Customer request.

3.1.9.1 Test restores are not subject to the SLA given in paragraph 6.3.

3.1.9.2 Test restores will be scheduled to begin within seven (7) days of the Supplier receiving the Customer's request.

3.1.9.3 Should a test restore require the allocation of any additional resources (for example, the temporary provision of extra storage to hold the restored data), the Supplier reserves the right to charge for these on a consumption basis.

3.2 The Supplier will not:

3.2.1 Provide backup support for any non-server client (e.g. mobile, tablet).

3.2.2 Provide direct data migrations involving other backup services.

3.2.3 Support backup of operating systems other than Windows and Linux.

3.2.4 Train Customer's staff on the use of the Service.

3.2.5 Provide end-user support.

4 Unmanaged Backup

4.1 Where the Order Form shows "Unmanaged Backup", the Supplier will:

4.1.1 Provide a secure storage vault of the contracted capacity within a data centre managed by the Supplier.

4.1.2 Deploy one or more DS-Clients into the Customer infrastructure.

4.1.3 Manage the DS-Client and the server on which it runs.

4.1.4 Store a secure copy of the Encryption Keys, unless the Customer specifically instructs the Supplier not to.

4.1.5 Enable malware scanning within the Service if the Customer has purchased it as a Service option.

4.2 The Supplier will not:

4.2.1 Create backup sets or backup policies.

4.2.2 Perform post installation configuration and backup set testing.

4.2.3 Perform data restores.

4.2.4 Provide backup support for any non-server client (e.g. mobile, tablet).

4.2.5 Provide direct data migrations involving other backup services.

4.2.6 Support backup of operating systems other than Windows and Linux.

4.2.7 Train Customer's staff on the use of the Service.

4.2.8 Provide end-user support.

5 Security

5.1 The DS-Client encrypts all backed-up Customer data during the backup process using a unique Encryption Key.

5.2 The Supplier will securely store a copy of the Encryption Key, unless the Customer expressly instructs the Supplier not to do so.

5.3 The Customer may keep its own copies of the Encryption Key in whatever manner it sees fit, and accepts sole liability for any results arising from its copies being compromised or stolen.

5.4 Should the Customer instruct to Supplier not to keep a copy of the Encryption Key, the Customer accepts sole liability for securely storing its Encryption Key, and accepts that its backed-up data will be forever lost should the Customer not be able to provide the Encryption Key when required.

5.5 The Supplier will not be liable for any loss suffered by the Customer in relation to any misuse or loss of the Encryption Key.

6 Service Levels

6.1 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; or • Failure of a single backup job	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

6.2 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.

Measure	Description	Value	Fee Credits
Service Hours	The hours during which the service and SLA is provided	24/7/365	
Platform Availability	% of the service hours during which service availability is guaranteed (excluding planned maintenance in paragraph **Error! Reference source not found.** below)	99.9%	Pro rata proportion of the Monthly Charges for any Non-Availability Period

6.2.1 "Availability" in this paragraph 6.2 refers to Availability of the Cloud Backup Service infrastructure only; loss of Service due to failure of any part of the Customer infrastructure or the Customer's internet connectivity is specifically excluded.

6.2.2 Platform Availability does not guarantee backup success; backup failure may occur for many reasons other than platform Availability and is thus not included in the Availability SLA.

6.3 The Supplier will use its reasonable endeavours to commence a data restore following a request from the Customer, within the Response Times as set out in the table below.

Event Type	Service Hours	Response Time
P1	24/7/365	Within 4 hours
P2	24/7/365	Within 8 hours
P3	Business Hours	Within 24 hours, measured during Business Hours
P4	Business Hours	No target SLA

6.3.1 Priority levels in this table align with Event Priority given in table 6.1 of this Schedule.

6.3.2 Time to complete a data restore cannot be guaranteed due to unknown factors such as quantity of data being restored; the SLA clock is paused when the restore starts and restarted when it finishes.

6.4 Where incidents are identified within the Cloud Backup Service, the Supplier shall not be liable for fixing these incidents where the Service is sold on a Unmanaged Backup basis and the fault lies in any part of the Service other than the backup platform infrastructure or DS-Client applications.

7 Fee Credits

7.1.1 Any Fee Credits which fall due pursuant to paragraph 6.2 above are payable subject to and in accordance with the terms contained in the Conditions.

7.1.2 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.

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

7.1.4 "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 6.2 above.

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