This Service Schedule for **Hosted Backup Services v8.0.0** (the "Service") marketed as "**RecoveryVault"** replaces all previously signed / incorporated version(s) of the Service Schedule(s) for Hosted Backup Services (if any) and forms part of the Master Services Agreement and Master Services Schedule. Its provisions are an integral part of the Master Services Agreement. Words and expressions defined in the General Conditions and Master Services Schedule shall (unless otherwise defined in this Services Schedule) bear the same meanings where used in this Service Schedule. In this Service Schedule the following words and phrases shall have the following meanings unless the context otherwise requires:

1. Interpretation

1.1. **"DS Client"** or **"DS Client Software**" means the data collector, which collects data to be protected on the LAN.

1.2. "**DS Client Minutes**" means the total number of minutes in a month, less all Scheduled Downtime, multiplied by the total number of DS Clients.

1.3. **"DS System"** means that SP data repository, where protected data is stored.

1.4. **"Native"** or **"Native Size"** means the original size of the latest generation of all data that the DS-Client has backed up (the **"Restorable Size of Data"**)**.** This includes restorable data that has been deleted from the source, but not from online.

1.5. **"Stored"** or "**Stored Size"** means the current actual physical size of all data that the DS-Client has backed up.

2. Service Overview

2.1. Hosted Backup Services provide access to one or more of the following:

2.1.1. Acronis™ backup and recovery technologies via a hosted cloud-based service.

2.1.2. Asigra™ backup and recovery technologies via a hosted cloud-based service.

3. Standard Features

3.1. Customers may select from one of the following: (1) **RecoveryVault Express Edition** – an agent based backup and recovery solution based on technology from Acronis™ which provides for offsite backup to a single SP datacentre and (2) **RecoveryVault Enterprise Edition** – a NIST FIPS140-2 certified, agentless backup and recovery solution for 80 (eighty) heterogeneous platforms based on technology from Asigra™ which provides for offsite backup replicated between two SP datacentres.

3.2. **Retention**

3.2.1. Backups may be retained for any period specified by the Customer provided the Customer maintains an active subscription.

3.2.2. SP shall have not retain backups beyond the duration of this Service Schedule.

3.3. **Support and supported platforms**

3.3.1. Support is not included as a standard component and is provided via one of the following for an additional fee: Service Level Agreement or Ad Hoc support billed hourly.

3.3.2. Note: The platforms listed as supported for RecoveryVault Express are subject to change by Acronis™ at any time without notice. Some limitations may apply. Refer to the User Guide at www.acronis.com/support/documentation/ for more details.

3.3.3. Note: The platforms listed as supported for RecoveryVault Enterprise are subject to change by Asigra™ at any time without notice. Some limitations may apply. Refer to the Support Matrix at www.asigra.com for more details.

3.4. **Encryption**

3.4.1. Both editions encrypt data in transit between the Customer environment and SP datacentre(s).

3.4.1.1. RecoveryVault Express supports 256-bit encryption of backups at rest. Encryption can be enabled per backup set by Customer.

3.4.1.2. RecoveryVault Enterprise enforces 256-bit AES encryption during processing, in transit and at rest, and has been certified as NIST FIPS140-2 compliant.

Initial

3.4.2. It is not the responsibility of the SP to create, maintain and safeguard user names and encryption keys. SP does not maintain any records in this respect. In the event of failure to safeguard the password and encryption key records for each licence, SP will neither be able to grant access to the server nor be able to decrypt the backup data.

4. RecoveryVault Express Edition

This is an agent based backup and recovery solution based on technology from Acronis™ which provides the following features:

4.1. **Laptop, workstation and server backup**

4.1.1. Intelligent file selection and exclusion facilitates rapid, transparent backups over low-speed and dial-up connections.

4.1.2. Byte-level patch incremental backups minimise data transfer by identifying only the changed bytes in modified files.

4.1.3. All data is compressed in transit and storage, further minimising transfer times, network loads and storage requirements.

4.1.4. Data can be recovered from any previously backed up state allowing file and system rollbacks.

4.1.5. Advanced scheduling allows multiple backups per day in one or more backup sets.

4.1.6. Definable Pre/Post backup and data-capture commands enable integration with other applications or temporarily stop services.

4.2. **Database protection**

4.2.1. Includes support for database aware backups of Microsoft Exchange, Microsoft SQL, Active Directory and Microsoft SharePoint.

4.3. **Virtual Machine data protection**

4.3.1. Support for VMware vSphere ESXi 6.0, 5.5, 5.1, 5.0.

4.3.2. Support for Microsoft Windows Server 2016 Technical Preview 4 with Hyper-V.

4.3.3. Support for Microsoft Hyper-V Server 2012/2012 R2, 2008/2008 R2.

4.3.4. Support for Microsoft Windows Server 2012/2012 R2, 2008/2008 R2 with Hyper-V.

4.3.5. Support for Microsoft Windows 10, 8/8.1 (x64) with Hyper-V.

4.3.6. Support for Citrix XenServer 4.1 - 6.5.

4.3.7. Support for Red Hat Enterprise Virtualization 2.2 - 3.5.

4.3.8. Support for Oracle VM Server 3.x.

4.3.9. Support for Linux KVM.

4.3.10. File level recovery and image based recovery in a single backup pass supported on VMWare and Hyper-V.

4.3.11. Support for image-based backups with seamless Oracle VM integration to capture your entire setup quickly and easily.

4.4. **Offsite storage of backed up data and local storage**

4.5. RecoveryVault Express stores the backed up data remotely to a single SP datacentre.

4.6. Backups can be optionally configured to enable local storage.

4.6.1. Local storage enables a copy of the backed up data to be saved on a storage location on the Customer LAN. This ensures that relevant backup sets are always available for immediate restoration at LAN speed.

4.6.2. Local storage helps address disaster restore requirements by saving copies of the backup files at a local storage location. If a restore is needed, the file can be restored quickly from the local environment, at LAN speed, without connecting over the internet to SP datacentre.

4.6.3. SP may provide an appliance which will act as a storage location. The fees associated with the provision of appliance(s) are specified in the Service Fee Schedule(s).

4.6.4. If no appliance is specified, SP shall be entitled to request that a storage location be provided.

4.7. **Mass Deployment**

4.7.1. The Mass Deployment feature enables deployment of the client software in silent mode and automatic software configuration.

4.7.2. Automated setup and installation reduces administration and support costs.

Initial

5. RecoveryVault Enterprise Edition

This is an agentless based backup and recovery solution based on technology from Asigra™ which includes all the features (unless otherwise specified) of RecoveryVault Express Edition plus:

5.1. **Agentless deployment via an on-site backup appliance.**

5.1.1. RecoveryVault Enterprise provides for offsite backup replicated between two SP datacentres, together with a cached copy on an SP provided and purpose built appliance.

5.1.2. This on-site backup appliance handles all the on-site processing of backup tasks and negates the requirement to install a software agent on every machine to be backed up.

5.1.3. This agentless architecture reduces the CPU overhead normally associated with backup agents deployed on target machines.

5.1.4. It also ensures that updates and maintenance to the backup and recovery solution does not require maintenance windows on the target systems being backed up.

5.1.5. The appliance can be configured in a fault tolerant N+1 configuration (*Windows only*) ensuring that backup operations are not affected by maintenance, patches or upgrades to the RecoveryVault appliance.

5.1.6. The on-site appliance is also used as a central store of Customer encryption keys to maintain FIPS 140-2 compliance.

5.1.7. The local cached retention policy can be configured to automatically manage the amount of data that is cached locally on the appliance.

5.2. **Automated Virtual Machine protection**

5.2.1. New guest Virtual Machines ('VMs') can be detected automatically.

5.2.2. Guest VMs can be automatically backed up according to a centralized backup configuration management policy.

5.3. **Virtual Machines Data Protection**

5.3.1. Support for VMware including VSphere 4, ESX 3.5, ESX 3.0, ESXi, Workstation and Server, vStorage API for Data Protection (VADP) and Changed Block Tracking (CBT).

5.3.2. Support for Hyper-V including Server, Cluster and Volume Shadow Services (VSS) writer.

5.3.3. Support for Citrix Xen including XenServer, XenDesktop and VM Protection and Recovery snapshots.

5.3.4. Support for Redhat KVM.

5.3.5. Support for Parallels including Virtuoso Containers, Server, Workstation and Desktop.

5.3.6. Support for Oracle host based backups.

5.3.7. Support for file level recovery and image based recovery in a single backup pass.

5.3.8. Note: File level recovery from within a virtual machine image backup is only supported for VMware images.

5.4. **Virtual disaster recovery**

5.4.1. Recover immediately from local machine failures - Local DS-VDR allows Customer to recover faster from machine outages by simply turning on a backup copy of the virtual machine in Customer local environment and continue business operations with little or no downtime.

5.4.2. Fail over to a warm VMWare spare in a remote data centre using Remote DS-VDR.

5.4.3. RecoveryVault Enterprise performs low-impact backups to minimize the use of storage, network and computing resources, while ensuring all backup data is always recoverable. It extends VMware's Change Block Tracking (CBT) features to both backup and restore ensuring rapid recovery using the least amount of resources.

5.5. **Continuous Data Protection ('CDP')**

5.5.1. When CDP is enabled, the changes to a specified data source are monitored; when changes are detected, data is automatically backed up offsite.

5.5.2. The client also provides automatic retention policy enforcement for regulatory requirements.

5.5.3. Retention enforcement is enabled for both regular and CDP backup.

5.5.4. Separate retention configurations can be established for both local and offsite data storage, and eliminate the accumulation of vast amounts of data requiring storage.

Initial

5.6. **Extended database protection**

5.6.1. Includes support for database aware backups of Microsoft Exchange, Microsoft SharePoint, Microsoft Active-Directory, Lotus Notes, Microsoft SQL and Oracle.

5.7. **Autonomic Healing Tool**

5.7.1. The Autonomic Healing tool addresses the problems of file corruption and increases the integrity of SP datacentre storage of Customer backup data on a subsystem called the DS-System. It continually monitors the DS-System Online Storage for data corruption. If corrupt data is found, it corrects it, removes it, or reports that a correction is needed. In medium or large data processing, file corruptions are almost inevitable. They may happen due to hardware failures, software applications, file system problems, connectivity problems, or insufficient resources. They may also result from unpredicted operations, methods, or behaviour.

5.7.2. Autonomic Healing checks (1) Online file headers: header ID, version, compression and encryption types, invalid library links, invalid file names, header size, (2) Directory metadata in DS-System Online Storage: header ID, version, invalid names, header size, (3) Library links for common files, (4) Delta generation consistency: file naming consistencies across online generations, session consistencies across generations, (5) File and directory consistencies in DS-System Online Storage: name and ID, directory location, and (6) Data integrity and restorability (checks for logical corruption and logical consistency).

5.7.3. Autonomic Healing can fix (1) completely corrupted files: deletes files affected and those that depend on them (delta generation) so that next backup will send a new master generation, (2) Inconsistent file or directory IDs, (3) Inconsistent directory locations, (4) Inconsistent file name within directories and Inconsistent file name across online generations, (5) Delta generation linking/reconstruction inconsistencies and (6) Inconsistent backup sessions (two generations of the same file in the same session).

5.8. **Cost per Gigabyte reduction over time**

5.8.1. RecoveryVault Enterprise edition has a number of enhancements designed to reduce the cost per gigabyte fees for backup as backup and recovery capacity grows over time:

5.8.1.1. Common File Elimination.

5.8.1.2. Adjustable compression algorithms.

5.8.1.3. Recovery License Model pricing (see paragraph 7 below).

5.8.1.4. Advanced retention policies.

5.8.1.5. Adjustable compression ratios.

6. File selection and backup frequency

6.1. File selection and backup frequency is specifically excluded from SP's responsibilities. Care should be taken to ensure that the correct files are selected and that backups are run on a regular basis. At the end of each backup session, a log is produced indicating the outcome of the backup process. SP will not monitor these logs or success / failure of backups.

7. Recovery License Model ('RLM')

7.1. **Description of the Recovery License Model**

7.1.1. Under the Recovery License Model ("**RLM**"), SP will charge Service Schedule Fees based on the combination of cost per Gigabyte of backup ("**Backup Cost**") and cost per GB actually used ("**Recovery Cost**").

7.1.2. Customer will always require an equal amount of backup capacity and recovery capacity. For this reason, SP combines Backup and Recovery Capacity into a single SKU for purposes of invoicing.

7.1.3. Recovery cost will be based on a Recovery Performance Score **("RPS")** from 0 to 10, where 0 represents the highest Recovery Cost and 10 represents the lowest Recovery Cost. The RPS is a number from 0 to 10 that is calculated based on the amount of data the Customer recovered in the previous measurement period, as a percentage of backup capacity. The score then corresponds to a cost per GB per month for recovery capacity.

Initial

7.1.4. SP's recovery tracking software (**"RT")** measures data recovery performance, and is used solely by SP to determine the Customer's Recovery Performance Score.

7.1.5. Customer will receive a score of 10 if SP's tracking software calculates the Customer's recovery usage in the previous measurement period to be less than or equal to 5% (five percent) of the Customer's backup capacity.

7.1.6. Customer will receive a score of 0 if SP's tracking software calculates the Customer's recovery usage in the previous measurement period to be greater than or equal to 25% (twenty five percent) of the Customer's backup capacity.

7.1.7. Between 5% (five percent) and 25% (twenty five percent) recovery usage, a 2% (two percent) increase corresponds to a reduction in Recovery Performance Score of 1.

7.1.8. At the outset, the Customer's Recovery Performance Score will be 0 (zero). SP will track the Customer's recovery usage and calculate a new score after the first 6 (six) months ("Initial Measurement Period") and again after 12 (twelve) months ("Second Measurement Period". Thereafter measurement periods, will be annual ("Subsequent Measurement Periods").

7.1.9. **By way of example:** If during the Initial Measurement Period, the Customer backed up 100TB of data and SP's RT measured Customer's recovery usage to be 19TB of data, then in the Second Measurement Period, the Customer's RPS would be 3 (three). Customer's total Recovery Cost during the Second Measurement Period would be the cost per GB per month corresponding to a Recovery Performance Score of 3 (three), multiplied by the total recovery capacity.

7.1.10. SP will continue to track Customer's ongoing recovery usage using the RT during Subsequent Measurement Periods and at all times following the Initial Measurement Period. Recovery Cost will be based on the Customer's actual percentage of total data recovered during the immediately preceding measurement period.

7.1.11. Customer acknowledges that the Recovery Performance Score, and thus the Recovery Cost, may fluctuate depending on their prior usage. At all times the maximum recovery price per GB per month applicable to a Customer, cannot exceed the price per GB per month corresponding to a Recovery Performance Score of 0 (zero). If the Customer did not engage in any actual data recovery during a measurement period, the Customer's Recovery Performance Score will be 10.

7.2. **Largest Recovery Event Waiver**

7.2.1. When calculating the Recovery Performance Score, SP will waive the single largest recovery event (as reported by RT) experienced by the Customer during the preceding measurement period.

7.3. **Advanced Scheduling of Disaster Recovery Drills**

7.3.1. Customer may purchase Disaster Recovery Drills (**"DR Drills**") capacity.

7.3.2. Any unused DR Drill capacity will expire at the end of each measurement period.

7.3.3. The conduct by Customer of any pre-scheduled DR Drills during any measurement period will have no impact upon the determination by SP of RPS score for any subsequent measurement period.

8. Service Availability

8.1. If the Service is unavailable it must be reported to the SP and acknowledged by SP.

8.2. The period of Downtime will calculated from when the fault is reported, SP has issued a fault report reference and has acknowledged this as a fault on the Service.

8.3. Following investigation and repair SP will advise the time that the Service was restored. This will be deemed to be the end of the Downtime unless the fix is not confirmed.

8.4. **RecoveryVault Enterprise Edition**

8.4.1. "**Downtime**" means any period of time when DS Clients are unable to access SP data centre to initiate a restore of a previously successful backup.

8.4.2. "**Monthly Uptime Percentage**" is calculated using the following formula:

Initial

$$\frac{\text{DS Client Minutes - Downtime}}{\text{DS Client Minutes}} \times 100$$

where Downtime is measured in DS Client Minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of DS Clients impacted by that Incident

8.4.3. Exclusions to Service Availability Guarantee:

8.4.3.1. Any incident which is the result of a failure on a DS Client.

8.4.3.2. Any incident lasting less than 15 (fifteen) minutes.

8.4.4. **Service Credit:**

Monthly Uptime Percentage	Downtime per month	Silver SLA Service Credit	Gold SLA Service Credit	Platinum SLA Service Credit
< 99.9%	43.8 minutes	No Credit	No Credit	25%
< 98 %	14.4 hours	No Credit	50%	
< 95 %	36 hours	100%		