Cloud Direct LiveVault Online Server Backup Service Level Agreement

Revision 4.0

Contents

1 Document Control

Please be advised, we reserve the right to change or amend this agreement from time to time. Please ensure that you are referring to the latest revision of the Cloud Direct LiveVault Online Server Backup Service Level Agreement available from the PROVIDE™ portal.

2 What is LiveVault Online Server Backup?

LiveVault Online Server Backup provides internet-based electronic vaulting for scheduled backup of customer-selected data and the restore or recovery of that data on demand. Backup schedule policies can be configured as frequently as every 15 minutes (referred to as Continuous Data Protection or CDP). When installed and used in accordance with the defined requirements and guidelines, LiveVault is able to protect applications, open files, open databases, system state and security information. LiveVault is managed through a web-based portal that shows the status of backup jobs, restore jobs and enables the set-up, modification and deletion of backup policies.

Data protected under this service is encrypted before transmission to the data centres and remains encrypted at all times until it is restored using AES 256-bit.

The LiveVault services covered by this SLA are:

- Flex Accounts
- 1TB 90-day plan

3 What is a Service Level Agreement (SLA)?

An SLA is a commitment to achieve a specific level of service. If this target is not achieved, the service provider will commit to compensating you based on previously established penalties. Consequently, a vendor willing to commit to an SLA is therefore confident in the reliability of the service.

Cloud Direct views an SLA as a two-way agreement in which you the Customer also acknowledge your responsibilities to ensure the smooth operation of the supplied Service.

In the critical area of electronic backup it is important that business users have a robust, cost-effective and above all, consistent level of service and performance.

4 What is behind Cloud Direct's SLA?

'Cloud Direct' is the trading name for On Direct Business Services Ltd. Specialising in cloud-based backup solutions, Cloud Direct are a leading broker of cloud services including disaster recovery, collaboration and protection tools, communication services including broadband and leased lines, VoIP telephony / unified communication solutions, and a range of hosted server and desktop platforms. Cloud Direct holds ISO27001 (IT Security Techniques) and ISO20000 (IT Service Management) accreditations for the provision and support of Cloud IT backup, security and disaster recovery services.

The datacentres used in conjunction with this service are also ISO27001 accredited, tier-3 status and are located within the European Union for all necessary data compliance.

5 What is offered by Cloud Direct's SLA?

Cloud Direct is committed to providing exceptional customer service at every opportunity and our key customer satisfaction measure is Net Promoter Score (www.netpromoter.com). Some aspects of the supplied service such as a high level of system availability should be taken as read. Our Service Team will endeavour to provide you with that 'extra mile' of service that, whilst not contractual, is what we believe you deserve.

The following sections describe our service level commitments and should be read in conjunction with our published Terms and Conditions (see www.clouddirect.net/legal for the latest version). This SLA may also be varied from time to time.

If you have any comments or observations about our performance and the service we provide you should contact our Head of Operations, Mark Gold on 0800 0789 438 or email mark.gold@clouddirect.net.

6 Data Location and Service Security

With LiveVault, you get peace of mind knowing that your data is backed up securely. LiveVault provides the following benefits:

6.1 Datacentre location

- Customer data is stored within the EU to comply with both the Data Protection Act and EU Data Protection Directive. This also complies with many professional standards but you should check the details of any of your associated standards to verify compliance. The primary datacentre is in London, UK and the secondary datacentre is in Amsterdam, Netherlands.
- Each datacentre is ISO 27001 and SOC2 accredited.

6.2 Datacentre features and redundancy

- Content is replicated from a primary data centre to a secondary data centre so replication is constant.
- Your data is stored in a redundant environment with robust backup, restoration, and failover capabilities to enable availability, business continuity, and rapid recovery. You will not be notified when failover occurs as typically failover does not result in service interruption.

6.3 Datacentre security

- These datacentres offer a number of physical and technology-based security features including 24/7 on site security, CCTV and encrypted servers.

6.4 Data transit and storage

- The data is encrypted when a backup is ready for transport to the datacentre using AES 256-bit encryption.
- The data remains encrypted during transit and storage to ensure security at all times.
- When you setup the service you are provided with an encryption key, please ensure you keep a record of your encryption key safe and do not forget it.
- Cloud Direct do not hold a copy of your encryption key, nor do we have access to your data at any time.

6.5 Service updates and patching:

- The service offers three different types of patching and updates which can include important security updates, fixes for software bugs and new functionality:
    - Some updates and patches are pushed out at the backend and implemented straight into the data vaults. There is no customer action required for this.
    - Some smaller break/fix updates are automatically updated on the agent. There is no customer action required for this.
    - Larger agent updates are put forward as a full agent update. In this scenario the Cloud Direct Technical Services team will contact you to advise you of the update and request you to download the new version.

7 Scope of Supply

Please make reference to your Sales Agreement for details of your specific purchased services. All of our LiveVault products come with 24/7 support via telephone and email as detailed below.

When your service is setup you will receive an encryption key for your data, please keep a copy of this safe. Without this key you will not be able to decrypt your data if you ever need to restore. Cloud Direct do not hold a copy of your unique encryption key.

To get your service running smoothly you will need to run an initial backup; which depending on the amount of data on your server and the available bandwidth, could take some time. You can assume an upload speed of approximately 2GB per day for each 256kbps of your available upload bandwidth. If you have a large amount of data, typically 100GB or more, you may require a data seeding service to quickly upload your data into our datacentres. This service is not included as standard. If you require or would like to discuss this additional service please contact the Cloud Direct Sales team on 0800 0789 437 to discuss your requirements in detail.

You may have decided to subscribe to a Turbo Restore Appliance (TRA) as part of your service, please make reference to your Sales Agreement for details. This enables you to have a local data cache which offers faster data recovery times. Set up correctly, this device can provide a range of automated reporting functions. Considering your data protection policies you must ensure that the storage does not go above 60% of the total device storage capacity, the remainder is required for system operation. You should have appropriate insurance cover in place for the value of this appliance as damage or non-recovery will be charged at replacement cost.

Internet-based data transmission and recovery will depend on many factors including your connection speed and quality, local internet usage, the rate of data change, and total Gigabytes involved. Your Sales Account Manager would have discussed your internet bandwidth with you to ensure the minimum speeds are available and to ensure you appreciate these factors. Bandwidth latency can have a significant effect on data transfer rates; detailed performance tables can be provided separately on request. You must ensure that you have the necessary internet bandwidth and server processing power to manage the level of data change involved, and especially the impact on your day-to-day operations if you are operating the continuous data protection (CDP).

Depending on the subscribed Service you will have selected from the following available retention periods: 30-day, 90-day, 1-year, 7-year and 1TB 90 day plan. Please make reference to your Sales Agreement for the retention period you have agreed to.

- Every backup taken within the last 24 hours is kept. If the backup schedule is set to CDP, there will be up to 96 versions from the most recent 24 hours, subject to size and change rate of files. If the policy is set to a nightly schedule, there will be only one.
- If CDP has been selected, see the below number of versions possible for each retention setting:

Retention Setting	Total amount of versions available	Version breakdown	Version deletion age
30 day	Up to 155	First 24 hours – 96 versions 7 days (every 6 hours) – 28 versions 31 days (every day) – 31 versions	Over 31 days
90 day	Up to 159	First 24 hours – 96 versions 7 days (every 6 hours) – 28 versions 31 days (every day) – 31 versions 4 months (one per month) – 4 versions	Over 91 days
1 year	Up to 167	First 24 hours – 96 versions 7 days (every 6 hours) – 28 versions 31 days (every day) – 31 versions 12 months (one per month) – 12 versions	Over 1 year
7 years	Up to 195	First 24 hours – 96 versions 7 days (every 6 hours) – 28 versions 31 days (every day) – 31 versions 12 months (one per month) – 12 versions 7 years (one per quarter) – 28 versions	Over 7 years
1TB 90 day plan	Up to 112	First 24 hours – 96 versions 7 days (every day) – 7 versions 5 weeks (every week) – 5 versions 4 months (one per month) – 4 versions	Over 91 days

Please be aware that not all of these versions will be available until you have used the service for the full retention period; for instance to get the full amount of versions on the 30 day retention, you will need to have used to service for 31 days.

Following expiration, your data will be securely deleted and no longer available to you. If you select a retention different from the subscribed service, Cloud Direct retain the right to revert to the subscribed terms without customer authorisation.

When configured, the system is able to send a range of system status reports and automated warning messages to nominated email addresses. A typical set up will send a warning email in the event of the server being disconnected from the data centre for more than four hours or the failure to produce a restorable data version after 18 hours of a scheduled backup. You should confirm the setup of this service with your IT Administrator or the Cloud Direct Support Team.

Restore performance will be influenced by the data type being restored (as data may have to be rebuilt from incremental changes gathered over time) and the internet connection. (For example, an 8Mbit/s bandwidth connection with an RTT (Round-Trip Time; length of time it takes for a signal to be sent plus the length of time it takes for an acknowledgement of that signal to be received) better than 50ms should be able to recover a maximum of 3GB of data per hour. If a large amount of data is to be recovered, it is possible to

request your data to be transferred onto a dedicated Media Restore Device which can then be shipped to a location you specify. This service will incur additional service and courier charges and should be ordered after discussion with the Cloud Direct Support Team.

8 Scope of Support

Cloud Direct are pleased to provide support for genuine technical issues and troubleshooting. This is where features of the product or service, or, the product or service itself can be demonstrated as not operating correctly or users are unable to access the services through approved platforms. Furthermore, Cloud Direct will assist with a range of administrative functions and activities that typically require an experienced administrative user.

As examples, we have provided some typical supported and unsupported scenarios.

8.1 Examples of Supported Scenarios

Examples of typically supported scenarios are:

- Password resets
- Failed backups
- Error messages
- Assisting with restores
- Single reinstallation when replacing hardware
- Investigating and addressing an instance of a service outage

8.2 Examples of Unsupported Scenarios

We will always endeavour to go the extra mile for our customers where we have the resources to do so. Our support philosophy is to resolve issues with a feature or function that is not operating correctly within its definition, as opposed to providing user training and support for working features. There is a wide range of excellent online help within the subscribed applications and also training materials on the Cloud Direct website;

Examples of typically unsupported scenarios are:

- Server operating system issues.
- Any issues you are experiencing with the application you are running on the server.
- Server issues including hardware failure, connection to the server from a desktop, etc.
- Support for any connectivity or networking problems (e.g. internet / router / firewall access) where those services are not purchased through Cloud Direct.
- NAS boxes.

9 Support Case Prioritisation

As outlined in the Cloud Direct Support Agreement, issues reported to us by customers are categorised into one of four levels: Standard, Moderate, High and Critical. We will assess and agree with you the criticality and impact of the issue on your business and assign an appropriate issue level, please see the below examples as indicators of how we will categorise your LiveVault issue if one should arise:

Standard	-	An issue that does not interfere with your business such as a request for a repeat invoice or support on how to do something relating to your LiveVault service.
Moderate	-	Assistance in recovering a non-business critical file or data.
High	-	An issue that results in an interruption to the service such as a failed backup or recovery of a business critical file.
Critical	-	A full disaster recovery scenario – you must make us aware of any such critical situation by phone to avoid delays.

10 Our Responsibilities

To provide you with an enterprise-class online backup service and the highest level of customer service as described in this SLA and your contract with us, we commit to:

- Contact you once the service is installed and check that you are happy with the service and all is working well. We refer to this process as 'On-Boarding'.
- Support you, at your request, with the selection of your protected data but the ultimate responsibility for data selection resides with you at all times.
- Provide free of charge updates to the service at regular intervals and inform you of specific requirements for upgrades.
- Maintain your data in a secure manner and will not provide access to your data without appropriate security checks being completed. If we are not convinced of a caller's right to access your account we will seek further clarification from a senior representative from your company.
- Ensure you can recover your protected data following a problem or incident at your company. Where possible, we will help with re-integrating your data into your company systems but our responsibility ends with recovery of your protected files and data. Our Support Team have the right to withdraw from providing further support if they believe they may be putting your systems at risk; or you lack the technical expertise required; or your request is outside the scope of our supply/support.
- Contact you at least once a year to seek your customer Net Promoter (satisfaction) Score and any feedback you may have. We will act on your feedback.
- Make your departure, should you choose to leave Cloud Direct, as smooth as possible and continue to support you until the end of the contracted term and assist where possible with account closure.

11 Your Responsibilities

To ensure we can effectively deliver your service we require your cooperation in the following areas:

- To provide a stable computer environment on which the service is installed and which meets the system operating requirements including sufficient internet bandwidth and latency performance. Before installation and any upgrades you will refer to any Installation, Release Notes and associated service documentation provided by Cloud Direct.
- In a Windows operating system environment the backup service relies on the Microsoft Volume Shadow Copy service (VSS). You are advised to ensure that you keep your operating system up to date with the latest service packs and patches as upgrades and fixes are released all the time and may affect your backup service performance and reliability.

- Service performance can be directly influenced by your internet bandwidth and latency. Service performance issues are normally the result of internet service interruptions and you should check this before contacting us.
- Before signing our Service Agreement you will check your equipment and operating system environment against the service minimum requirements.
- You are responsible for ensuring that all the data you wish to be protected has been selected for inclusion in the service. You will undertake regular checks that all your required data is being protected.
- You are responsible for selecting the appropriate retention level as detailed in your Sales Agreement, any failure to do so could result in you being charged for the extra retention service. We also retain the right to revert to the subscribed terms without customer authorisation.
- You will retain a secure note of your encryption key required for any form of data recovery.
- It is your responsibility to respond to any system status or warning messages received and maintain the appropriate email addresses in the system control portal to receive these.
- You will undertake test restores at appropriate regular intervals to ensure that you can recover your critical data and systems and inform Cloud Direct Support Team of any issues encountered.
- In the event of data recovery using the service, you must have access to the appropriate level of technical knowledge to rebuild your data into your systems (if you do not have this skill yourself, you should use an IT partner or IT support company). You should appreciate the difference between the recovery of single data files, the recovery of an email database system (such as Exchange), the limitations of System State recovery, and the possible need for comprehensive disaster recovery of an entire server. Our Support Team can advise on these matters.
- If you have opted to rent a Turbo Restore Appliance on your premises, you must include this within your insurance cover. Any appliance that is damaged or that is irrecoverable will be charged at its replacement cost.
- To ensure your use of the Service does not affect the operation of the overall service platform. In the event that your usage is adversely affecting the overall platform, it may be suspended or terminated without liability to Cloud Direct upon prior written notice (or immediately without notice in the event of a technical emergency).
- You will notify us of your desire to cancel the service, giving the appropriate notice, as described in our Terms and Conditions.

Please refer to our full Terms and Conditions at http://www.clouddirect.net/legal for a complete breakdown of both your and our contractual responsibilities.

12 Service Availability and Financial Claims

We commit to our customers that the LiveVault service will have an uptime of 99.9% and above (excluding planned maintenance and the web portal). This is worked out over a month. To calculate the uptime of a service use the following formula:

$$\frac{\text{Total number of minutes in a month} - \text{Minutes Downtime}}{\text{Total number of minutes in a month}} \times 100$$

Service Downtime is measured from the time a case is raised with us by you until the LiveVault service is restored.
Any rebate will be prorated based on number of affected users.

This SLA does not apply to any performance or availability issues in conjunction with:

- Factors outside of our control
- As a result of your or third party services, hardware or software
- Your use of the service after you were advised by us to modify your use and did not do so
- Being on a trial of the service
- An unauthorised action or inaction by you or your employees, agents, contractors, vendors or anyone gaining access to the LiveVault network through your passwords or equipment
- Your failure to adhere to any required configurations, supported platforms and outlined policies for acceptable use. This includes any changes made during the service such as changing your operating system.
- Reserved licences which have not been paid for at the time of the downtime

If the uptime falls below 99.9% for any given month, you may be eligible for the following rebate:

Online service availability in a given month (excluding planned maintenance)	Rebate (% of per affected User monthly recurring charge)
Less than 99.9% and greater than or equal to 98.0%	10%
Less than 98.0% and greater than or equal to 95.0%	20%
Less than 95.0%	30%

If you wish to make a claim for non-conformance against this SLA you should do so in writing to support@clouddirect.net citing your reasons in full, the duration of the downtime, the number of users affected and relevant Cloud Direct Support Case numbers within 10 calendar days of the online service interruption.

Our Directors will review any incident raised by evaluating all the information reasonably available to them and make a good faith judgment on whether a Rebate is owed. You must be in compliance with our contractual agreement and this SLA in order to be eligible for a Rebate. If we determine that a Rebate is owed to you, we will apply the Rebate to your next invoice; you may not offset the Rebate yourself from any payments owed. If you receive an SLA Rebate this is your sole and exclusive remedy for any performance or availability issues for any LiveVault service covered by this SLA.