Cloud Direct Backup Pro (Attix5) Service Level Agreement

Revision 1.0

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 making reference to the latest revision of the Cloud Direct Backup Pro Service Level Agreement available from the PROVIDE™ portal.

2 What is Backup Pro?

Backup Pro (previously known as Attix5) provides internet-based electronic vaulting for the scheduled backup of customer-selected data and the restore or recovery of that data upon request. Data to be protected is selected including data from network shares. Plug-ins are available to protect specific applications, databases, network drives and system information. When installed correctly and used in accordance with the defined requirements and guidelines, Backup Pro is able to protect applications, open files and databases and registry and security information from both the local machine and approved and tested network drives. As well as protected data being transferred to two offsite data centres, a local copy of the last backup is held on the client computer or server providing quick network restores if required. The Backup Pro service is managed through a local application on the client computer or server that shows data protected and the status of backup and restore jobs. For multiple user installations, a management application is also available for controlling a community of users. 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 Backup Pro services covered by this SLA are:

- PC Licences
- Mac Licences
- Server Licences
- Unix and Linux Licences
- Additional Plug-ins

3 What is a Service Level Agreement (SLA)?

An SLA is a legally binding commitment to achieve a specific level of service. If this target is not achieved, the service provider will commit to compensating the customer based on previously established penalties. Consequently, a vendor willing to commit to an SLA is confident in the ability of the service and therefore creates customer reassurance.

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.

Cloud Direct supports Backup Pro technology delivered by Restor. The Backup Pro service is ISO27001 accredited. 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 Backup Pro, you get peace of mind knowing that your data is backed up securely. Backup Pro 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 Directive, this service in particular offers UK only datacentres. This 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 Essex, UK and the secondary datacentre is in Hertfordshire, UK.
- Each datacentre is Tier-3 and ISO 27001 accredited.

6.2 Datacentre features and data 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

- The physical security, access and redundancy of the datacentres have the following controls:
  - 24/7 on site security.
  - Restricted entry to the buildings are maintained through on site security guards and electronic key-card access. Only authorised personnel are permitted to access the datacentre.

  - Building wide monitored CCTV.
  - Each data centre is fully secure and operates with a system of backup generators and UPS to cope with any power fluctuations and outages.
  - Fully automatic and centrally monitored Argonite fire suppression systems and environmental control systems are installed in each data centre.

6.4 Data transit and storage

- The data is encrypted when a backup is compiled and again, when it 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 a new agent you are prompted to create an encryption key, please ensure you keep a record of your encryption key safe and do not forget it. You can change your encryption key, but you need to input your existing encryption key to do so.
- 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

- New versions and patches are automatically set to update on your service and requires no customer action. This is done to ensure you are able to utilise the latest features and security updates as soon as they become available.
- For some updates, particularly those that will bring about a large amount of change, the Cloud Direct Technical Services team will contact you to advise you of the update and co-ordinate the rollout of the new version.

7 Scope of Supply

Please make reference to your Sales Agreement for details of your specific purchased services. All our Backup Pro 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 it. 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 you have on your server/computer 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 50GB 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 this additional service please contact the Cloud Direct Sales team on 0800 0789 437 to discuss your requirements in detail.

We recommend that you do not exceed 400GB of data for selection per Backup Pro licence. Please be aware that large volumes of data that are backed up will result in a long restore times.

The Backup Pro service has an optional local cache space to provide a fast restore of the last backed up data. If employed, you will need to leave between 1.5x and 2x, of the size of your protected information as free disk space for the cache environment. The Local Data Cache and Backup Pro System Working Directories must be on the local computer or server and not stored on remote or network drives.

Internet-based data transmission and recovery will depend on many factors including your connection speed and quality, local internet usage, rates of data changes, and total Gigabytes involved. Your Sales Account Manager would have discussed your internet bandwidth with you to ensure the minimum bandwidth is 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 computer or server processing power to manage the level of data change involved and especially the impact on your day-to-day operations.

The Backup Pro service is typically setup to complete one backup at the end of the day, however, it can capture file changes down to an hourly frequency; this is subject to data volume and rate of change coupled with local computer processing capability. At any time, daily versions of files are available for a minimum of 30 days to a maximum of 60 days with 1 month end roll-up. You should assume there will always be 30 versions from daily backups together with a version from the last month. This includes any data that is deselected from the backup set. Following expiration, data will be securely deleted and no longer available to you.

When correctly set-up with a working SMTP mail service, Backup Pro is able to send an automated non-backup warning message (or a backup successful message) to nominated email addresses. It is your responsibility to respond to these messages and maintain the appropriate email addresses in the system application. You should confirm the setup of this service with your IT Administrator or the Support Team.

It is normally fine to select and backup data residing on a NAS device providing the Backup Pro service has permissions to read the data and the device remains permanently attached. It is important that any system local data cache, working folders, or Backup Pro plugin folders are not held on a NAS device. NAS drives can come in many different types and performance characteristics – from high performance units to much cheaper, consumer-grade equipment. Due to this wide performance range it is important that customers undertake their own backup tests and restores to ensure reliable operation. Cloud Direct recommend the business grade QNAP devices if required.

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 USB hard disk which can then be shipped to a location you specify. This service will incur additional 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
- 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:

- Operating system issues.
- Any issues you are experiencing with the application you are running on the server.
- Any issues not pertaining the service purchased from Cloud Direct such as 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.

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 Backup Pro 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 Backup Pro service.

Moderate - An issue such as degraded service performance where the service remains operational but at a reduced level.

High - An issue that results in an interruption to the service such as a failed backup or recovery of a single 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 product 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.
- 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 will retain a secure note of your encryption key required for any form of data recovery. Cloud Direct do not keep a copy of your unique encryption key.
- 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 Service 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). To ensure that you keep the automated email

warning system up to date with an appropriate email address and to contact the Cloud Direct Service Team in the event of repeated system warnings.

- 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 Backup Pro service will have an uptime of 99.5% and above (excluding planned maintenance). This is worked out over a month. To calculate the uptime of a service use the following formula:

$$\frac{\text{Total number of minutes in a month – Minutes Downtime}}{\text{Total number of minutes in a month}} \quad \text{x 100}$$

Service Downtime is measured from the time a case is raised with us by you until the Backup Pro 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 Backup Pro 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 99.5% 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 99.5% 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 Backup Pro service covered by this SLA.