Centre Technologies
16801 Greenspoint Park Drive Suite 200
Houston, TX 77060
Ph: 281-506-2480 **Fax:** 281-763-2355

Service Level Agreement (SLA) for CBaaS™ (Centre Backup-as-a-Service)

1. OVERVIEW

This exhibit represents a Service Level Agreement ("SLA") between Centre Technologies, Inc. ("Centre", "Service Provider") and Customer for the provisioning of IT services required to support and sustain C-BaaS Services.

2. SERVICE AGREEMENT

The following detailed service parameters are the responsibility of Centre in the ongoing support of this Agreement.

2.1. **Service Scope**

The following Services are covered by this agreement:

- C-BaaS provides an automated and unattended backup service ensuring that data held on desktops, laptops, smartphones, tablets, physical and virtual machines application / database servers third party and cloud-based applications is securely backed up and transferred offsite to be stored, encrypted in Centre's datacenter
- Centre's agentless backup and recovery solution eliminates server disruptions and minimizes maintenance windows.
- The C-BaaS DS-CLIENT software needs to be installed on a physical or virtual server as a standalone or in an on-demand grid within the Customer's LAN. Using standard APIs, the C-BaaS DS-CLIENT captures requested data within the LAN and securely transfer it to Centre's datacenter.
- Backed up data is transferred encrypted (NIST FIPS 140-2 Validated) from the central site, laptops and remote sites (Remote Offices/Branch Offices - ROBO) to Centre's datacenter.
- Utilizing the concept of incremental forever, C-BaaS leverages block-level deduplication and compression to transfer only changed data from Customer's Central/ROBO to Centre's datacenter.
- Bandwidth throttling enables bandwidth optimization and backups even in cases where certain remote locations might suffer from low connection speeds
- C-BaaS provides an easy to use interface that simplifies the backup and recovery process and provides detailed information about scheduled operations.
- Centralized configuration of the C-BaaS DS-USER enables a network administrator/IT manager to specify exactly what data is to be backed up ensuring investment is not wasted by backing up unauthorized or unnecessary information.
- A user-defined number of backup versions of files are retained on disk for immediate recovery
- Service is remotely monitored 24 hours a day, seven days a week by Centre staff, and alerts are provided if scheduled backups are not completed or errors occur after 3 consecutive backup failures.
- Disk to Disk solution enables backed up data to be easily recovered without the need to locate and identify backup tapes.
- Clients can perform regular recoveries, allowing them to test the integrity of their data at any time.
- A Centre Crash Response Team is on stand-by 24 hours a day, seven days a week to support major data recovery by delivering requested backup data to the client site based on this SLA. The client is responsible for any time and materials required to deliver requested backup data including but not limited to storage devices, storage arrays, network attached storage appliances, express delivery service charges, etc.
- In the event of a major client site Disaster, a portable storage media device is delivered to the client site, to a specified Disaster Recovery site or a restore to virtual environments is performed at Centre's facility via remote terminal access. The client is responsible for time and materials required to deliver requested backup data including but not limited to storage devices, storage arrays, network attached storage appliances, express delivery service charges, etc. A nominal monthly fee may apply for this optional level of coverage; emergency rates may apply for any use of compute, storage and network resources in Centre's Cloud environment, billed in standard calendar month increments.
- C-BaaS DS-CLIENT can be configured with a local storage option for fast recoveries. In this scenario if a recovery is needed, data stored locally can be quickly retrieved at LAN speed, without connecting through the IP WAN to the C-BaaS DS-SYSTEM. Local storage can be configured for specific backup sets, especially ones containing critical data
- 24hrs/day x 7 days/week x 365 days/year Help Desk support is provided.

3. C-BAAS SERVICE DEFINITION

C-BaaS is a unique Disk to Disk alternative to traditional backup methods, replacing conventional tape-based systems with a fully automated cloud backup and recovery solution. It provides agentless, centralized and automated backups of desktops, laptops, smartphones, tablets, physical and virtual machines, application / database servers and third party-based cloud applications with secure offsite storage and immediate recovery from either a local or cloud copy.

The C-BaaS DS-CLIENT is installed onto the Client network and performs the backup and recovery activity.

3.1. C-BaaS DS-Client

The C-BaaS DS-CLIENT are self-contained processing units that assist in the delivery of the C-BaaS Service.

C-BaaS is delivered through a suitably configured C-BaaS DS-CLIENT installed on the client's network. The C-BaaS DS-CLIENT configuration will be determined by the specific requirements of each client.

The key criteria in establishing the specification of the C-BaaS DS-CLIENT are the size and scope of the client network, the number of client servers, the mix of applications and operating systems, and the quantity of data to be managed.

3.1.1. C-BaaS DS-CLIENT and C-BaaS DS-USER GUI

The C-BaaS DS-CLIENT software runs as a service on Windows platforms or as a daemon on Linux platforms. It serves as a gateway to Centre's DS-SYSTEM. The client's data tagged for backup flows through the C-BaaS DS-CLIENT, where it is deduplicated, compressed and encrypted before being sent to Centre's DS-SYSTEM.

Each C-BaaS DS-CLIENT is connected directly to the client's Local Area Network (LAN). The client is responsible for providing an appropriate IP address. The C-BaaS DS-CLIENT supports either static or DHCP generated addresses.

Using standard APIs, the C-BaaS DS-CLIENT can remotely capture requested data and transfer data to Centre's datacenter.

The C-BaaS DS-CLIENT comes by default with the ability to backup a wide range of applications and databases including: Windows 2000/2003/2008, Windows Vista/XP, Microsoft SQL Server, Microsoft Exchange, Microsoft SharePoint, Microsoft Outlook, and Oracle (including SAP-certified backup/restore). In addition, C-BaaS can backup data residing in third party cloud apps like Salesforce and Google Apps, DB2, MySQL, PostgreSQL, Sybase, GroupWise, VSS-support, System State & Services Database, Netware, AS/400, Linux/Unix, Mac OS X and Android. C-BaaS DS-CLIENT integrates natively with VMware, Hyper-V and XenServer virtual machines servers.

The C-BaaS DS-CLIENT is configured and operated using a separate interface called C-BaaS DS-USER. The C-BaaS DS-USER GUI can be installed on one or more of the clients' Windows, Mac OSX, Linux Red Hat or Suse systems.

The C-BaaS DS-USER is the clients' interface with the C-BaaS DS-CLIENT and can be installed on the same C-BaaS DS-CLIENT appliance or in a LAN workstation or laptop.

The C-BaaS DS-USER GUI is operated by the Authorized Client Network Administrator to define backup sets and schedules, monitor backups, and perform restores.

C-BaaS DS-USER GUI access is integrated into Windows, Linux and UNIX networking security. Individual user accounts, or groups of users, can be defined and granted authority to perform different levels of C-BaaS Service functions.

Typically, apart from the C-BaaS DS-USER GUI and the C-BaaS DS-CLIENT, no other C-BaaS software is installed on the client's systems, making this an Agentless solution that is particularly easy to deploy and support.

3.1.2. Encryption Keys

For the security of clients' backed up data, the C-BaaS Client Software installed in the C-BaaS DS-CLIENT encrypts every file it sends with an encryption key provided by the client. The files are stored and remain encrypted on the C-BaaS DS-SYSTEM at all times. The decryption process occurs during recovery and is performed by the C-BaaS DS-CLIENT. This ensures that all backed up data transferred and stored outside the client location is always encrypted. The C-BaaS DS-CLIENT uses up to 256 AES encryption and can be configured with private and account encryption keys.

Encryption meets National Institute of Standards and Technology (NIST) FIPS 140-2 compliance and has been validated by NIST with Certificate #1240.

3.1.3. Private Key

The private key is the default encryption key. It is used by the C-BaaS DS-CLIENT to encrypt data before it is transmitted to the C-BaaS DS-SYSTEM at the Centre datacenter. Backup files that are unique to a C-BaaS DS-CLIENT are encrypted using the C-BaaS DS-CLIENT private key and stored in the C-BaaS DS-CLIENT private library area on the C-BaaS DS-SYSTEM.

3.1.4. Account Key

For clients with more than one C-BaaS DS-CLIENT, an account encryption key is also defined. The account key is used to encrypt client files that are common to multiple C-BaaS DS-CLIENT to the same C-BaaS DS-SYSTEM. These common backup files are encrypted with the account key and stored in the account library area on the C-BaaS DS-SYSTEM. C-BaaS DS-CLIENTs that share a C-BaaS DS-SYSTEM must be configured with the same account key.

The C-BaaS DS-SYSTEM uses encryption cookies to verify every connection by the C-BaaS DS-CLIENT. Cookies are a piece of code generated using the encryption key. The C-BaaS DS-CLIENT sends its cookie on every connection request. The C-BaaS DS-SYSTEM compares it with the cookie originally received during the initial C-BaaS DS-CLIENT configuration. This verification process ensures integrity of both private and account keys. After initial configuration the authentication between the C-BaaS DS-CLIENT and the C-BaaS DS-SYSTEM is transparent.

Both private and account encryption keys can be up to 32 alpha/numeric characters and are configured during C-BaaS DS-CLIENT installation. Encryption keys are stored in the Database in encrypted form, so even if you have full access to the C-BaaS DS-CLIENT (such as Centre Client Support) they cannot be read. Intentional or unintentional changes to the encryption keys will make data stored on the C-BaaS DS-SYSTEM unusable.

It is the responsibility of the client to supply appropriate values for the private and account encryption keys.

IMPORTANT: The client is responsible for storing their original encryption keys in a secure location. Loss of the keys will prevent recovery of the C-BaaS DS-CLIENT and the client's backup data. Centre has no knowledge of the client's encryption keys and is unable to recover them. The encryption keys can be sent to the C-BaaS DS-SYSTEM in an encrypted format, and through the DS-Operator a file can be generated to restore the C-BaaS DS-CLIENT.

3.1.5. C-Baas DS-CLIENT SLA Dashboard

Centre has an SLA Dashboard for monitoring C-BaaS DS-CLIENT backup and recovery related service levels agreed between the parties. It is HTML-based and accessed from client machines running TCP/IP and an appropriate Web browser (Microsoft Internet Explorer, Mozilla Firefox or equivalent).

The SLA Monitor graphical user interface provides status information about the C-BaaS Service (and reference information about Centre client services). The C-BaaS Status Report displays the current status of all C-BaaS backup activity. It includes backup start and completion times, backup results, a list of backed up data and information on any open files that failed to back up.

3.1.6. C-BaaS Service Setup

Centre will arrange a convenient time to perform the installation and configuration of the C-BaaS DS-CLIENT. Once the C-BaaS DS-CLIENT has been installed, Centre will work with the client to configure the C-BaaS Client Software. This will involve configuration of the C-BaaS DS-CLIENT settings, definition of the clients' encryption keys, installation of the C-BaaS DS-USER GUI and demonstration of the C-BaaS functionality.

One day of onsite support for this initial configuration is included within the standard C-BaaS Service offering. The client can purchase additional onsite support at a fixed daily rate.

4. C-BAAS OPERATIONS

All C-BaaS operations are performed using the C-BaaS DS-USER GUI. Authority to perform C-BaaS operations can be controlled by defining access to authorized users or groups of users, thus preventing backup and restoration of data by unauthorized personnel. Centre reserves the right to prevent or deny access to the modification of backup and restoration operations including but not limited to configuration of backup and/or restore jobs and global configuration options.

4.1. Backups

C-BaaS backups are based on backup sets that define the scope of the backup operation to be performed. Backup sets perform the specified backup operation and can be executed manually or scheduled automatically.

4.1.1. Backup Sets

A backup set defines the files or databases that are to be backed up. They can include or exclude files and databases by directories, or by filtering the file type. This allows the Client Administrator to define backup sets that meet the client's precise requirements, thus eliminating the backup of unnecessary data.

In addition, these backup sets define the number of retained generations, or versions, of files and databases that have been backed up. This enables the client to selectively restore any of the previous versions of files that have been backed up. The default number of generations is set during installation.

Multiple backup sets can be defined for the same client system. This feature enables the client to define separate backups of different types of data on the same system. Multiple backup sets for the same system can also be setup independently.

Backup sets are defined in a similar manner regardless of the type of system to be backed up. A single interface enables efficient administration of the C-BaaS Service.

Authorized administrators can manually execute ad-hoc backups. However, under normal conditions execution of backup sets are scheduled and performed automatically.

4.1.2. Backup Lifecycle Management

C-BaaS provides for the long-term storage of non-critical backup data. This is typically backup data no longer required for day-to-day operations, but required for peripheral business concerns, such as legal, compliance or audit purposes.

The long-term retention of backup files, also known as Backup Lifecycle Management (BLM), is performed by defining and executing additional backup sets for the appropriate client file or database systems. These long-term storage backup sets are typically executed on a monthly or quarterly cycle and complement the regular day-to-day backups.

4.1.3. Backup Schedules

C-BaaS has an extensive, calendar-based scheduler for automatically executing backup sets. Schedules can be defined to execute backups daily, weekly, monthly, or at a more randomly defined frequency.

Multiple schedules can be defined, and multiple backup sets can run on a single schedule. Where multiple backup sets are run on the same schedule, the client network administrator can define the number of concurrent backup sets to be executed, and the priority in which they should be executed.

The C-BaaS DS-USER GUI provides a graphical view of the backup schedules. This allows the client network administrator to quickly view the status of the backups and identify any conflicting or overlapping schedules.

4.1.4. Monitoring Backups

In addition to the C-BaaS DS-USER GUI, a web-based interface from the C-BaaS DS-CLIENT presents daily management reports on the status of the C-BaaS Service. This web interface includes a summary of scheduled backups, highlights of any errors that may have occurred and statistical information detailing the quantity of data backed up.

The C-BaaS DS-USER GUI provides extensive monitoring and reporting capabilities for client administrators. This includes detailed logs of backup activity, details of all files backed up, error reports, and audit trails for all backup and restore activity.

4.1.5. Initial Data Collection

The primary method of backup is over the WAN circuit between the C-BaaS DS-CLIENT and the C-BaaS DS-SYSTEM at Centre's datacenter. However, in situations where the initial backup volume makes a network transfer impractical, Centre will perform an initial backup on a portable drive and transport the physical media to the Data Center.

Where it is appropriate for Centre to manually transport the initial backup data, the process will involve connecting a removable/portable hard-disk location on the client premises to the C-BaaS DS-CLIENT via a LAN connection. Initial backups are performed to this removable/portable hard-disk location until a mutually agreed-upon time when the removable/portable hard-disk device is disconnected from the LAN and transported back to the Data Centre. Once at the Data Center, the data residing on the removable/portable hard-disk device is imported into the C-BaaS DS-SYSTEM and incremental backups between the C-BaaS DS-SYSTEM and the C-BaaS DS-CLIENT can occur on a regular basis (either scheduled or on-demand).

The initial backup is the only circumstance where a full backup is performed, after which, all other backups are incremental (incremental forever).

4.2. **Recoveries**

The C-BaaS DS-USER GUI allows the authorized client network administrator to quickly and easily select and recover data. The administrator can restore data to a remote system by using their desktop/laptop.

There are four methods in which data can be restored.

- Data is restored at LAN speed from Local Storage.
- Data is restored across the WAN link.
- Restore data is delivered via a portable disk.
- A C-BaaS DS-SYSTEM with replicated data can be delivered to the client's site or alternative disaster recovery location or hot-site in the event of a major DR scenario.

The following table maps the 4 different categories of data restoration methods.

Data Restoration Methods				
Category	**Description**	**Volume of Client Data**	**Restore Method**	**RTO (Hours)**
1	**Local Recovery** Fast recovery from local storage	N/A	Local Storage	Depends on amount of data to be recovered at LAN speed
2	**Moderate Data Loss** Single/small number of files; small/medium server	Up to 5GB	Cloud Storage	Depends on amount of data to be recovered at WAN speed
3	**Major Data Loss** Major database server or multiple servers	From 1GB to 1TB	Portable Disk Restore	< 48 Hours, excluding national holidays
4	**Disaster Recovery** Multiple server loss or complete site	1TB+	DS-System Restore	< 120 Hours, excluding national holidays

Local Restore

Local Restore addresses fast recovery requirements by saving copies of the backup files at a local storage location. If a recovery is needed, the file can be restored quickly from local storage, at LAN speed, without connecting through the IP WAN to the C-BaaS DS-SYSTEM. Local storage can be configured for specific backup sets, typically ones containing critical data. On the first regular backup, the entire backup set is stored in the local storage.

When a file in a backup set identified for local storage is created or modified, it is sent by the backup process to both the C-BaaS DS-SYSTEM and to local storage. Data stored locally is compressed but not encrypted, and stored as regular generations, without elimination of common files or delta processing. However, delta processing is performed to the data before it is sent to the C-BaaS DS-SYSTEM. Any backup sets marked for local storage are also sent to the DS-System to be stored encrypted and compressed with master/delta online generations and common file elimination.

Requests to recover data will attempt to retrieve data from local Storage first. If the requested files are not available locally, data will be retrieved from the C-BaaS DS-SYSTEM storage.

Utilizing local storage on DS-Clients speeds up the recovery process thus increasing SLA compliance. In addition, local storage facilitates backup windows to be met regardless of WAN connection bottlenecks.

Local storage is not required but strongly recommended. Centre can provide local storage to facilitate strict SLAs for a nominal monthly fee should the client need or require this option.

Cloud Restore

(Normally conducted by the client without Service Provider intervention)

The C-BaaS DS-USER GUI provides a Restore Wizard that guides the client administrator/end user through the process of selecting and restoring data. The Restore Wizard allows the administrator to search and select files for restore, select the version of the files and choose the target destination for delivery.

Having selected the data to be restored, the C-BaaS DS-CLIENT retrieves the data across the WAN from the C-BaaS DS-SYSTEM at the Centre datacenter facility. The C-BaaS DS-CLIENT then sends the data to the specified system on the client network. As part of the operation, all associated security permissions for the data are restored.

In case backup data is available in the C-BaaS DS-CLIENT Local Storage, data will be restored by C-BaaS DS-CLIENT at LAN speed. The C-BaaS DS-CLIENT then sends the data to the specified system on the client network.

This speed at which the data is restored depends largely on the amount of data to be restored and the available speeds of WAN connections. This method is primarily used for smaller data restore operations.

Portable Disk Restore

(Normally conducted by both the Client and Service Provider)

For larger quantities of data, the client administrator can invoke the Disaster Recovery Wizard to request that a copy of the backup data be copied to a portable disk device.

The Disaster Recovery Wizard provides the same level of restore granularity as the Restore Wizard, but rather than restoring the data across the network it is copied to a portable disk device, which is then transported to the client site. The client network administrator can then use the C-BaaS DS-USER GUI to restore the requested data directly from the C-BaaS DS-CLIENT to the system being restored.

The only data that can be restored from the portable disk device is that which was specified when initially requested. If additional backup data is required then this can be restored either online or by initiating a new request for a portable disk device.

The client is responsible for time and materials required to deliver requested backup data including but not limited to storage devices, storage arrays, network attached storage appliances, express delivery service charges, etc.

Restore from a new replicated C-BaaS DS-SYSTEM (Normally conducted by both the Client and Service Provider)

The fourth restore scenario refers to shipping a new C-BaaS DS-SYSTEM with replicated data to the client's site or hydrating the data, using the bare metal restore options of the C-BaaS software engine to boot the environment in the Centre Cloud environment. This could be used as an alternative to the portable disk device, or in a major disaster situation, where complete backup data is required.

Centre can replicate the production C-BaaS DS-SYSTEM entirely to a new C-BaaS DS-SYSTEM and ship it to either the client's primary work site or an alternate disaster recovery location as defined by the client. The replicated C-BaaS DS-SYSTEM is then connected to the client's private LAN connection. Data can then be restored in the same way as would an online restore but with the performance benefit of the replicated C-BaaS DS-SYSTEM being on an internal LAN at native Ethernet speeds.

The client is responsible for time and materials required to deliver requested backup data including but not limited to storage devices, storage arrays, network attached storage appliances, express delivery service charges, etc. A nominal monthly fee may apply for this optional level of coverage; emergency rates may apply for any use of compute, storage and network resources in Centre's Cloud environment, billed in standard calendar month increments.

4.3. **Service Availability Measurement & Credit & Termination**

4.3.1. **RTO.** Should the RTO fall below the threshold set for a given month per Restore Category, Centre will provide a Service Credit as noted in the chart below:

Recovery Category	RTO Service Level Threshold	Service Credit*
3	RTO Met	0%
4	RTO Met	0%
3	RTO Exceeded	10%
4	RTO Exceeded	15%

** Service Credit issued against the Monthly Recurring Charge (MRC) paid by Customer for C-BaaS Services requires the Customer to have followed best practice recommendations for recovery categories 1 and 2.*

4.3.2. **Service Credit.** A Service Credit awarded in any calendar month shall not, under any circumstances, exceed Customer's MRC.

4.3.3. **Unused Service Credit.** Any unused Service Credits existing upon termination of the Agreement shall lapse without reimbursement to Customer.

4.3.4. **Termination Without Penalty.** In the event that Customer receives Service Credits hereunder of 15% or more in any two consecutive months or in any three months in any rolling twelve month period, then Customer may terminate and discontinue the Centre Hosted Services prior to the end of the Service Term without penalty by notifying Centre Technologies within fifteen (15) days following the end of the applicable calendar month.

4.4. **Service Availability Claims**

4.4.1. **Service Claim.** Customer must provide all reasonable details regarding the Claim, including but not limited to, detailed description of the incident, the duration of the incident, the number of affected users, the locations of such users, and any attempts made by the Customer to resolve the incident.

4.4.2. **Service Claim Submission.** Customer must submit the Claim to Centre by the end of the month following the month in which the incident which is the subject of the Claim occurs.

4.5. **Service Availability Exclusions**

4.5.1. **Force Majeure**

The period of time when Services are not available as a result of Scheduled Downtime; or
The following performance or availability issues that may affect Services:

a. Due to factors beyond Centre's reasonable control, including, without limitation, acts of any governmental body, war, insurrection, sabotage, embargo, "Acts of God" (i.e.…fire, flood, earthquake, tornado, etc.), strike or other labor disturbance, interruption of or delay in transportation, failure of third-party software or inability to obtain raw materials, supplies or power used in equipment needed for provision of the Service Level Agreement;
b. That resulted from Customer's or third-party hardware, software, or services;
c. That resulted from actions or inactions of Customer or third parties;
d. That resulted from actions or inactions by Customer or Customer's employees, agents, contractors, vendors, or anyone gaining access to Customer's network by means of Customer's passwords or equipment;

4.6. **Service Definitions**

4.6.1. **"Downtime"** means a period of time when Customer is unable to read or write any Service data for which they have the proper authority.

4.6.2. **"Claim"** means a claim submitted by Customer to Centre pursuant to this SLA that a Service Level has not been met and that a Service Credit may be due to Customer.

4.6.3. **"Incident"** means any set of circumstances resulting in a failure to meet a Service Level.

4.6.4. **"Service Credit"** is the percentage of the monthly service fees for the Service that is credited to a Customer for a validated Claim.

4.6.5. **"Service Level"** means performance standards mutually agreed to by the Parties that measure the level of service provided specifically set forth herein.

4.6.6. **"Scheduled Downtime"** means pre-approved maintenance windows or times where Centre notifies Customer through the Centre Change Control Procedure and Change Control Form of downtime needed for network, hardware, Service maintenance or Service upgrades at least 72 hours prior to the start of such Downtime.

5. SERVICE MANAGEMENT

5.1. **Service Hours**

Coverage parameters specific to the service(s) covered in this Agreement are as follows:

Telephone Support: 24 x 7 x 365	Email Support: 24 x 7 x 365