

DATA PROTECTION SERVICE LEVEL AGREEMENT

This Data Protection Service Level Agreement ("SLA") is incorporated into the Quote executed by C Spire Business and Customer for Data Protection Services and sets forth the specific terms and conditions under which C Spire Business shall supply the Data Protection Services described herein to Customer. The general terms applicable to such Services are contained in the Master Terms and Conditions ("MTC") and the Master Service Level Agreement ("MSLA") incorporated into the Quote by reference. Capitalized terms used but not defined herein shall have the meanings set forth in the MTC and MSLA.

Contents

Terminology	2
Service Description	2
Service Offerings	2
Managed Image-Based Server Backup	2
Cloud Connect	3
Disaster Recovery	3
Unmanaged Disaster Recovery	4
Managed Disaster Recovery	5
Disaster Recovery Service Level Metric	8
Workstation/Endpoint Backup Service	9
Data Protection Service Availability Dependencies	9
Data Protection Service Limitations	11
Service Delivery Additions	12

Terminology

These are service specific definitions. Common definitions are already defined in our Master Service Level Agreement.

- **Backup Agents** – An agent-based backup requires the installation of software, known as an agent, on each machine that needs to be protected. In agent-based backup, a service, daemon or process runs in the background to facilitate the backup.
- **Recovery Point Objective (RPO)** – The amount of time going backward where data will be consistent between the production environment and the virtual environment. RPO determines how much utilization is needed on the network.
- **Recovery Time Objective (RTO)** – The amount of time it takes after a disaster to get the environment back up and running in full production. The timer for this objective begins when C Spire support acknowledges a declaration of a disaster by the customer, not at time of failure or through any automated monitoring.

Service Description

C Spire Business Data Protection Services deliver comprehensive protection of your business-critical data assets and can offload the labor and burden of managing, monitoring, and supporting your backup and replication infrastructure to our team of trusted and reliable experts. We offer backup and replication solutions that are scalable and flexible to fit your specific needs.

Service Offerings

Managed Image-Based Server Backup

Cloud-based backup and recovery for physical and virtual servers. Designed to protect system image-level data. In the event of a restoration need, C Spire Business can restore individual files or the entire system from backup. For dedicated/single tenant environments, requires an on-site primary backup appliance.

- For Customers who want to back up to onsite systems, backups are sent to a local appliance, which can be leased through C Spire Business.
- If offsite copies of those backups are needed, Customers can add an offsite backup option (see Cloud Connect).

- For Customers who require backups within C Spire Business Cloud Infrastructure, no backup appliance is needed.

Features

- **Backup Agents:** With Managed Data Protection, C Spire Business will install backup agents for the Customer, configure jobs and retention schedules.
 - The Backup Agent provides the communication to the master server, which controls backup/restore scheduling and other backup/restore functions. In addition, the backup Agent initiates the transport of the data across the network from the client's Server to the C Spire Business storage device.
- **Retention Schedules:** Retention schedules will be defined based on Customer needs. Standard options are 7-day, 14-day, and 30-day.
- **Job Definition:** C Spire Business will capture an entire image of the system on a regular schedule. Customer is responsible for notifying C Spire of additions or deletions of servers requiring backup services.
- **Restore Services:** C Spire Business will be responsible for restoring data within the requirements of this SLA. Customer will bear responsibility for service and applications functionality. C Spire Business reserves the right to bill customer at standard rates for providing additional assistance relating to a restoration request.
- **Encryption:** Data is encrypted at rest. The data is visible and accessible by any C Spire Business backup administrator.
- Customer data contained within a backup job that has expired or has exceeded defined retention cannot be recovered.

Cloud Connect

Cloud Connect offers an offsite, remote copy of image-based backups. Cloud Connect targets exist in C Spire data centers and through our Partners with Wasabi Object Storage, Microsoft Azure and AWS. Offsite copies have separate licensing, retention schedules, and storage consumption from the primary local backups.

Disaster Recovery

Disaster Recovery refers to a process for quickly reestablishing access to business-critical systems in the event of a catastrophic event. C Spire Business' Disaster Recovery model provides a means for customers to securely replicate their production virtual environment to an offsite environment and allows for these replicated systems to be brought online with restore points updated within minutes or

seconds from the time production services were affected. Once running, reverse replication can be enabled to ensure resources can be easily transferred back to the Customer's production environment.

C Spire Business Disaster Recovery solution also allows Customers to conduct a planned migration of a production environment and fail back to that production environment. This would constitute a live failover and will incur normal daily resources charges as described in signed agreement. C Spire Business requires a minimum of 14 business day notice for any Managed Disaster Recovery Customer's planned failover event (test failover or live failover) to ensure proper support personnel is allocated and available to support your Disaster Recovery testing. Disaster recovery test support is limited to 8 hours and does not include supporting changes to the production environment.

Disaster Recovery testing may incur additional charges if additional time or capabilities outside of recovering the VMs are required.

Unmanaged Disaster Recovery

With the Unmanaged option, the Customer provides space in their VM or Hyper-V environment to host the required agents and management console. The Customer also manages the setup and management of their Disaster Recovery environment. C Spire Business provides the target environment and licenses.

- C Spire Business will provide installation software and instructions and guidance for the Customer to install any required services into the Customer owned/managed environment.
- C Spire Business will configure all target environments and assist the Customer with proper configurations related to our Disaster Recovery service.
- C Spire Business will provide support for the Customer to ensure the Customer's virtual environment is properly replicated and will assist with initial test failover to ensure systems do properly failover into the Customer's isolated test environment.
- The Customer will update/upgrade necessary Disaster Recovery software as required by C Spire Business and will maintain software versions within specified range compatible with C Spire Business' target environment.
 - In the event the pushed upgrade fails, the Customer may be removed from C Spire's Disaster Recovery system until such time as required customer upgrades are performed
 - C Spire Business will inform the Customer of any removal or disconnection from the Disaster Recovery environment to ensure timely upgrade is performed and loss of service is minimized as much as possible
- The Customer will be responsible for monitoring replication status and verifying
 - C Spire Business will provide first level support and troubleshooting to help resolve replication issues

- The Customer will initiate failovers in a test scenario. Live failover scenarios will require notification to C Spire Business to initiate.
 - C Spire Business will provide first level support and troubleshooting as necessary to ensure replicated VMs are successfully failed over and brought online to a running state in the DR environment
- Any change in servers applicable to the DR Service (additions, removals, etc.) must be performed in conjunction with C Spire Business and all applicable service fees will apply. The Customer must ensure that all applicable servers are properly licensed through the Disaster Recovery service.
- Customer is responsible for all applicable charges that may be incurred through a test or live failover scenario, including those applicable to the DR environment.

Specific Availability Dependencies

- The Customer is **required** to maintain the Disaster Recovery software versions as specified by C Spire Business. Failure to comply with this dependency will result in termination of Disaster Recovery replication services until remedied by the Customer.
- Sufficient network connection is needed from the Customer site to C Spire Business to sustain Customer VM data change rate replication.
- Service requires suitable network bandwidth for transport in some cases. C Spire Business reserves the right to limit availability of Service, even if a suitable network transport exists between C Spire Business and Customer Server.
- The RPO/RTO must fit within the technical limitations of the network connection, the daily data change rate and the required storage for data and journals.

Managed Disaster Recovery

C Spire Business will install and manage the Disaster Recovery licenses and platform in the Customer environment and will configure RPO and Journaling targets. Customer is responsible for developing and test application runbooks. C Spire is responsible for recovering the operating system.

Basic Requirements:

- C Spire Disaster Recovery Service as the replication service
- Storage space to house replicated VMs
- Managed Firewall in Disaster Recovery Environment
- Two Domain Controllers in Disaster Recovery Environment
- Failover testing once per Calendar year, limited to eight (8) hours

Limited Scope of Engagement: The Service Provider's obligation to provide fixed-fee Managed Services is strictly limited to the primary production environment. The Disaster Recovery environment is considered an unmanaged asset unless otherwise specified in a separate Statement of Work or Executed Agreement for management of the Disaster Recovery environment.

Billable Support & Application Recovery: All labor associated with the Disaster Recovery environment—including troubleshooting, falls outside the scope of the Agreement. Specifically, any labor required to bring up, validate, or troubleshoot applications is classified as a Professional Service billed on a Time and Materials (T&M) basis. Consequently, these specific application-level activities are not subject to any guaranteed Service Level Agreement (SLA) or Recovery Time Objective (RTO).

Responsibility Boundary & Networking: The Service Provider's recovery responsibilities end immediately when the Operating System is online and successfully verifies connectivity to the internet and local network. Any network infrastructure changes required to facilitate this connectivity (such as routing updates, VPN tunnel reconfiguration, or firewall adjustments) are expressly outside the scope of service and will incur additional charges on a Time and Materials basis.

Service Transferability

- **Failover Support:** Production managed services are non-transferable. Support within the DR environment is billed as time and materials.
- **Conditions for Permanent Migration.** Permanent migration of production services to the DR environment requires a formal contract amendment. Existing production service agreements do not automatically transfer to the DR environment. Upon execution of the amendment, Monthly Recurring Charges (MRC) may be increased to align with the specific costs of the DR infrastructure. Customer may exercise this migration option a maximum of one (1) time per contractual year.

Service Deliverables

- C Spire Business will install and configure any Warm Site or Hot Site Equipment (Data Center Colocation rates or other infrastructure, service and hourly rates may apply).
- Customer will provide C Spire Business with proper access into their environment and will provide any systems and access required for configuration of the service.
- C Spire Business will install the required Disaster Recovery software and licenses into the Customers' environment.
- C Spire Business will work with the customer to configure VPG as needed. Runbooks will be defined by the client and will document Client's failover process.

- C Spire Business will work with the Customer to develop a recovery plan and configure Virtual Protection Groups accordingly. Once C Spire Business has verified that the systems are running properly and completed a successful failover test of a virtual machine, the Service will be considered active, and billing will commence.
- C Spire Business will perform failovers at Customer request upon declaration of disaster or scheduled testing. A failover will ensure that the environment is active, IP configuration is complete, and communication within the disaster recovery environment is successful. All applicable charges for active recovery environments or changes in production environments will apply.
 - C Spire Business will **not test or troubleshoot** Customer-owned applications.
 - C Spire Business does not maintain application-specific runbooks.
 - Application support is billed as time and materials.
 - **Testing:** Failover testing will be limited to 8 hours once per Calendar year and is required for RTO metrics. Additional testing will be billed as a Time and Materials service.
- C Spire Business will update/upgrade necessary Disaster Recovery software as required to maintain software versions within specified range compatible with C Spire Business' target environment.
- C Spire Business will initiate failovers on behalf of the Customer for test or live failover scenarios and ensure servers are online and accessible during failover events.
- C Spire Business will utilize its standard monitoring software in conjunction with scripting and vendor provided APIs to monitor the Customer's SLA. C Spire Business will work with the customer to ensure replication targets are met.
- C Spire Business' Disaster Recovery Software maintains and calculates a customer's SLA as defined by their Journal Targets and RPO settings withing the software.
- Any change in servers applicable to the DR Service (additions, removals, etc.) must be performed in conjunction with C Spire Business and any and all applicable service fees will apply. **The Customer must ensure that all applicable servers are properly licensed through the Disaster Recovery service.**
- Customer is responsible for all charges that may be incurred through a test or live failover scenario, including those applicable to the DR environment, service fees, or other charges as may apply.

Specific Availability Dependencies

- Sufficient network connection is needed from Customer site to C Spire Business to sustain Customer VM data change rate replication.

- Service requires suitable network bandwidth for transport in some cases. C Spire Business reserves the right to limit availability of Service even if suitable network transport exists between C Spire Business and Customer Server.
- This RPO/RTO timeframe must fit within the technical limitations of the environment architecture, network connection, the daily data change rate and the required storage for data and journals.
- C Spire Business is not responsible for Customer-owned hardware, software, applications, or network. Customer is responsible for ensuring these are configured appropriately.
- If additional configuration work is required due to limitations of the Customer Network or other server/application requirements, C Spire Business reserves the right to bill Customer at current hourly rates. Reinstallation or reconfiguration of any systems due to such circumstances may be deemed billable.
- C Spire Business is **not** responsible for and **will not be obligated** to provide any support of or assistance in configuration, installation, administration, troubleshooting, maintenance, or repair of any Customer equipment and software, or integration of such equipment and software into the Customer network.
- Customer shall be responsible for any travel expenses incurred by C Spire Business in the course of providing any onsite service(s).

Disaster Recovery Service Level Metric

Service availability and Service performance goals are determined on a customer-by-customer basis outlined by the agreed upon RTO and RPO.

RPO is dependent on available bandwidth and data change rates.

The minimum RTO for failover server availability is four (4) hours contingent upon Customer performing successful annual Disaster Recovery testing. Without successful completion of annual testing, all RTO is "best effort."

RTO Scope Limitation: The expressed Recovery Time Objective (RTO) for C Spire Business applies strictly to the Service Provider's defined responsibilities (restoring the Operating System to an online state). Any delays caused by factors outside the Service Provider's direct control—including Client-managed network infrastructure, third-party vendors, or application-specific validation—are excluded from the RTO calculation. RTO calculation is contingent upon Customer performing successful annual Disaster Recovery Testing. Without successful completion of annual testing, all RTO is "best effort."

IP Addressing Requirement: Valid RTO execution and successful DR testing are contingent upon the Disaster Recovery environment utilizing different IP addresses (and subnets) than the Production

environment. The Client acknowledges that attempts to retain Production IP addresses in the DR facility (stretched networking) prevent timely routing updates. Consequently, if the DR strategy requires identical IP addressing, the RTO guarantee is voided.

Workstation/Endpoint Backup Service

This service requires the customer to also purchase End User Support.

User-level file backups that allow non-technical users to access and restore data without IT intervention quickly and easily. This service provides cloud storage, continuous backups, and browser access at the individual desktop level.

This service is not actively managed by C Spire Business. C Spire Business will provide customer with initial setup and configuration of agents on supported devices. Customer is expected to ensure workstation connectivity to the client network and agent connectivity to the backup service.

C Spire will provide basic remote support as a component of End User Support. Any on-site or additional remediation services will be subject to standard Professional Services hourly rates, including travel, time, and materials.

Workstation Backup Dependencies

- Client internet access to the network.
- Providing access to the server & existing backups.
- Operating System actively supported by the vendor.
- Customer workstation must be connected to the network for the duration of the backup process to ensure backup copy is completed.

Data Protection Service Availability Dependencies

The availability of Service is dependent on the following:

- Existence of a suitable network transport from C Spire Business to User(s). C Spire Business also reserves the right to limit Service availability in the event that necessary Service Components are either unavailable or unattainable at a reasonable cost to C Spire Business.
- The maximum size of any single file the Service can support on a Protected Server is equivalent to the maximum supported file size of the client file system.
- Job Scheduling is managed on a per customer instance.
- Initial Backup Time Requirements – The Initial Backup process for each Protected Server must complete before a Protected Server is fully protected. This process may take several days. Data

transfer rates for the initial Backup cannot be reliably estimated. Typically, if inadequate bandwidth is available for the given capacity, it could take many days, even weeks, to complete the Initial Backup. Customers can add the Backup Seeding option, which may drastically reduce this time. See Service Options above for more information.

- Machines backed up must have an Operating System under a current vendor supported.
- Firewall rules or other customer environment configuration may be required to support backup and restore or replication activities.
- Adequate network connection speeds must be available (depends on volume of data to be backed up or replicated).
- The configuration settings of certain outbound ports that must be open in order for transport to take place.
- VMware backups require the VMware environment to be functioning.
- Appropriate disk space must be available on the System drive (usually C: drive).
- An appropriate window of time must be allotted to complete the backup (depends on volume of data to be backed up).
- C Spire Business requires Customer to maintain a suitable standard of equipment that sufficiently supports the normal operation of our backup or replication applications.
- Customer must have sufficient bandwidth to transfer the daily change data within the specified backup window.
- It is Customer's responsibility to ensure that all users are able to connect to the Service and are configured properly. This includes, but is not limited to, Ethernet switches, Ethernet cabling, workstations, servers, operating systems, and software.
- The customer is responsible for providing C Spire Business up-to-date information on the location of the data to be backed up and the devices on which the backup agent should be installed. C Spire Business should be notified immediately of any changes to the location of data.
- Customer is responsible for ensuring the following client-side configuration requirements are in place:
 - VSS is properly enabled on Microsoft servers.
 - Appropriate disk space is available on the System drive (usually C: drive).
 - Adequate network connection speeds are available.
 - Appropriate window of time allotted to complete the backup (depends on volume of data to be backed up).

Data Protection Service Limitations

The following limitations apply to this Service:

- In unmanaged environments, the Customer is required to maintain the Data Protection software versions as specified by C Spire Business. Failure to comply with this dependency will result in reversion to Best Effort support for replication services until remedied by the Customer.
- C Spire Business reserves the right to discontinue or not to render managed backup services if our ability to perform said work is impaired by the Customer or any third-party creating circumstances beyond our control.
- Customer is responsible for Source File Integrity. This includes, but is not limited to:
 - Anti-virus/Anti-malware/Anti-ransomware protection of the source data
 - Updating the Operating System and Applications
 - Establishing appropriate security perimeter for infrastructure
- C Spire Business is not responsible if a backup is performed on a corrupted source.
- Customer must maintain original installation media and licensing for all software in the event reinstallation is required. C Spire Business will not be liable for application data loss or third-party data recovery service costs.
- The Data Protection Service is designed to provide service to server Operating Systems. C Spire Business reserves the right to refuse delivery of service to equipment deemed outside the target of the product such as, but not limited to, mobile devices, home users, and equipment other than servers.
- Protected devices must have Operating Systems under mainstream support from the Operating System vendor. If the Operating Systems fall outside of mainstream support, C Spire Business reserves the right to terminate any and all data protection services to the device.
- If Server is on network but not within a C Spire Business data center, then Customer will be responsible for supplying suitable environment for Server(s) and providing connectivity from Server(s) to nearest C Spire Business network point. If Customer network gear is not managed by C Spire Business, then Customer will be responsible for ensuring that Server(s) can communicate with the C Spire Business backup platform. If Customer network gear is wholly managed by C Spire Business, then C Spire Business will be responsible for ensuring that Server(s) can communicate with the C Spire Business backup platform.
- During Standard and Planned Maintenance Windows, restore operations and backup operations are not possible.
- Bare metal restores to new hardware are not included. This service only includes recovery to virtualized environments.

- Restore of servers/data into sandbox (isolated) environment for compliance testing, etc. is not included in the Managed Image-based Backup Service. Sandbox isolation for testing is available within the Disaster Recovery Service.
- Continued daily cleanup of storage or troubleshooting of inadequate storage to accommodate backups is not included.
- With unmanaged services, upgrades to local backup software/service are not included, and Customer must maintain version compatibility with C Spire Business's Data Protection service. Failure to maintain version compatibility will result in termination of data protection services to the affected device(s) or environment.

Service Delivery Additions

Upon receipt of the signed Quote, C Spire Business will provision one or more of the following for the Data Protection Service as required:

- C Spire Business install RMM agent depending on the Customer's specific Service configuration.
- C Spire Business will install and configure Backup Agents or replication depending on the Customer's specific Service configuration.
- C Spire Business will define and create backup or replication jobs based on input provided by the Customer, including data selections, job scheduling, job frequency, and backup retention time frames.