Cloud Backup and Recovery Service Terms

1. CLOUD BACKUP AND RECOVERY SERVICES

1.1. Definitions

"**Activation**" refers to the notification provided by one of Customer's designated representatives to Sungard AS indicating that an Event has occurred.

"**CDR Form**" refers to the document used to capture Customer design requirements and information.

"**Cloud Repository**" refers to the offsite copy of the local repository (storage used for backup) provided by Sungard AS.

"**Event**" refers to any planned event or condition that renders Customer unable to use the Protected Servers for their intended computer processing and related purposes.

"**Multiple Activation**" refers to when one or more other Sungard AS customers declare an Event at the same time as Customer.

"**Protected Servers**" refers to the physical servers and virtual machines receiving Managed Cloud Backup Services in connection with the quantity of data identified in the Order.

"**Recovered Servers**" refers to Customer servers to be recovered to a disaster recovery environment as specified in the Order.

"**Resources**" are the facilities, equipment, network and other resources used to provide the Services identified on the Order.

"**RPO**" is the recovery point objective, which is the age of the files or data in backup storage required to resume normal operations if a computer system or network failure occurs.

"**RTO**" is the recovery time objective, which is the maximum acceptable amount of time since the last data recovery point.

"**Test"** refers to the use of the whole or part of the Resources by Customer for disaster recovery testing purposes.

1.2. Cloud Backup

1.2.1. Features

Sungard AS will provide the following, in accordance with the completed CDR Form, for the data storage amount identified in the Order:

- Online access to the cloud disk system containing Customer's copy of backup data located at the Delivery Location ("Cloud Repository")
- Monitoring and management of the Cloud Repository

1.2.2. General

Customer will:

- Provide Sungard AS with the information necessary to adequately determine the infrastructure required to store the data including, but not limited to, the number of servers and the quantity of data to be backed up
- Obtain Internet or other IP bandwidth from Sungard AS or a third-party provider that is adequate to support a daily average replication RPO desired by Customer

- Procure, install and maintain any software and hardware at the Customer location necessary for the delivery of the Services identified in the Order
- Manage the retention of backup data to the Cloud Repository for the lesser of the time period stated in the CDR Form or the Term of the Order
- Be responsible for the security of Customer backup data transmitted and stored using the Services
- Restore the backup data located on the Cloud Repository

Customer is responsible for the quality and integrity of its data.

Customer is responsible for copy and/or recovery failures resulting from Customer maintenance, Customer use of or changes to retention or copy procedures, or Customer-owned infrastructure or application failure.

Within thirty (30) days after termination of the Order, Sungard AS will delete all Customer data from the Cloud Repository without any additional notification to Customer, unless Customer elects to migrate its data pursuant to the provision below.

Customer will notify Sungard AS sixty (60) days prior to termination of the Order if Customer wants its data to be migrated from the Cloud Repository to Customer's designated infrastructure. All data migration requests are subject to Sungard AS and vendor approval and will incur additional charges. Customer remains responsible for payment of the Monthly Fee as indicated in the Order, even after the termination date, until completion of the data migration is confirmed in writing by Customer to Sungard AS. Promptly following Customer's confirmation that the data migration has been completed, Customer's data will be deleted from the Cloud Repository.

Any resource use, including, but not limited to, server count, CPU, memory, storage or items contracted in the Order, in excess of the committed amount will result in the additional usage fee stated in the Order.

1.3. Managed Cloud Backup Services

1.3.1. Features

If identified in the Order, in addition to Cloud Backup Services, Sungard AS will provide the following for the Protected Servers in connection with the quantity of data identified in the Order:

- Installation and configuration of the Sungard-AS-provided backup software (including agents, if applicable) in accordance with Sungard AS' standard backup policies and the CDR Form
- Definition of backup methodology for virtual environments, databases and applications
- One initial data restoration test of a single file to a Customer-provided server
- Retention of backed-up data for the lesser of the time period stated in the Order or the Term of the Order
- Monitoring of detected backup failures and subsequent remediation and re-performance
- If identified in the Order, replication or storage of backed-up data offsite at the frequencies identified in the CDR Form
- Monthly reports identifying the backup job, restoration and, if applicable, replication success rates

1.3.2. General

Customer will:

- Provide Sungard AS with the information necessary to determine the infrastructure needed to back up the data including, but not limited to, the number of Protected Servers and the quantity of data to be backed up
- Provide Sungard AS with connectivity and administrative-level user access to Protected Servers as necessary for Sungard AS to perform Managed Backup Services

- Provide at least two dedicated network interfaces for backup and management of each Protected Server
- Provide sufficient disk space for data restoration
- Provide required backup hosts for virtual environments
- Comply with Sungard AS' Backup Policy, which is available for reference in the Customer Portal
- Customer will comply with the third-party vendor licensing terms and conditions, as applicable to the software package

Data restoration requests for reasons other than data loss or corruption are limited to the number identified in the Order. Additional requests may incur additional fees as identified in the Order.

Due to backup size and associated bandwidth requirements, Sungard AS does not guarantee that full backups will be scheduled on a particular day, that they will be completed within scheduled backup window(s) or that data restoration will occur within a defined time period. Sungard AS is not responsible for backup or recovery failures caused by Customer maintenance, Customer failure to adhere to Sungard AS' Backup Policy, Customer use of or changes to Sungard AS' backup scripts or procedures, Protected Server, Customer infrastructure or Customer application failure.

Sungard AS' standard daily backup window begins at 6PM in the time zone where the Protected Servers are located and ends at 6AM in the same time zone on the following day.

Incident resolution is limited to the backup infrastructure and is dependent upon Customer having provided dedicated management and administrative access.

If Customer requires encryption, Customer is responsible for encrypting its backed-up data using Customer-provided and retained passwords for encryption key generation.

1.4. Cloud Backup and Recovery Services

1.4.1. Features

If identified in the Order, in addition to Cloud Backup and/or Managed Cloud Backup Services, Sungard AS will provide the following in accordance with the CDR Form for the number of Recovered Servers identified in the Order:

- Recover the selected servers indicated in the Order to a disaster recovery environment
- Configuration of the initial recovery plan set up on Customer's protected environment, including fine tuning of the plan set up using a Sungard-AS-performed recovery
- Manage the replication and recovery of the Recovered Servers
    - Recovered Servers will have decreased performance during a Recovery Test or Activation, but performance will improve over time
- Remote access to Customer's Recovered Servers and data recovered from the Delivery Location to the disaster recovery environment identified in the Order during a Recovery Test or Activation
- Upon Customer request, analysis of the bandwidth between the Recovered Servers and the Sungard AS infrastructure required to support replication of Customer's data
- Commercially reasonable efforts to assist with the failback of Customer data from the disaster recovery environment to the production servers following an Activation
- Deletion of any Customer data and applications from the Recovered Servers following the conclusion of a Recovery Test or Activation

1.4.2. General

Customer will:

- Provide Sungard AS with the information necessary to determine the infrastructure required to recover the server including, but not limited to, the number of Recovered Servers and the quantity of data to be recovered
- Configure the VPN connection where the Recovered Servers are located
- Provide Sungard AS with the access necessary to install and monitor agents on Recovered Servers, conduct bandwidth analysis, install patches and upgrade the installed software agents
- Comply with Sungard AS' Change Management Policy, which can be reviewed on the Customer Portal, and related changes to the Recovered Servers (i.e., patches applied, upgrade of software, changes in IP address, etc.)
- Obtain Internet or other IP bandwidth from Sungard AS or a third-party provider that is adequate to support the daily average replication RPO based on the applicable recovery time Service-Level Objective ("SLO") and/or Service-Level Agreement ("SLA") listed below
- If necessary for Sungard AS to provide the Services described in the Order, Customer will provide an adequate number of infrastructure resources and virtual machines ("VMs")
- Maintain OSs and hypervisor software versions, if applicable, as supported by Sungard AS, and the underlying replication technology software (Sungard AS will provide Customer with a notice if the software must be upgraded or modified, and Customer will promptly upgrade such software following receipt of Sungard AS' notice)
- Ensure that its hardware and software related to the Services comply with technology vendor best practices to enable Sungard AS to achieve the SLO and/or SLA set forth below
- Have primary responsibility for the failback of Customer data from the disaster recovery environment to the production servers following an Activation

Data restoration requests attributable to data loss or corruption are included. Any additional requests may incur Managed Services hourly fees at the Committed Rate indicated in the Order.

Customer will provide its Activation notice to Sungard AS in the manner described in the Sungard AS Alert & Disaster Activation Guide (the "Guide"). Sungard AS will provide access to the Guide at time of implementation. For purposes of this Service, all references in the Guide to a "Disaster" shall mean an Event.

If Sungard AS' bandwidth analysis indicates that the amount of bandwidth specified in the Order will not support Customer's stated RPO, Customer will have the option to contract for additional bandwidth or Sungard AS shall be entitled to make an adjustment to the stated RPO to an RPO it reasonably deems achievable with such bandwidth.

One or more other customers may declare an Event and require use of the same Resources (including the Virtual Resource Pool) at the same time as Customer ("Multiple Activation"). "Resources" are defined as the facilities, equipment, network and other resources used to provide the Services identified on the Order.

The following provisions are intended to avoid or minimize contention for Resources during a Multiple Activation. Customer access to and use of Resources that are not then being used by other customers with previously declared Activations will be determined by their contracted recovery tier as follows:

- Customer's contracted-for recovery tier will be set forth in the Order. Sungard AS will maintain records of its receipt of Activations, which will be the exclusive basis for determining the order in which Activations are declared.
- Customer may use the Resources for 30 days following an Activation. If an Event continues for longer than the 30-day period, Customer may continue to use the Resources for an incremental Daily Usage Fee.
- For Pay-Per-Use resources, Customer agrees to pay the daily rate set forth in the Order for Resource Pool usage following an Activation or Recovery Test.

- Customer will comply with Sungard AS' Test Scheduling & Cancellation Policy. All Recovery Tests are subject to immediate cancellation by Sungard AS if and when any other customer declares an Event and requests use of the Resources being tested. Any such cancelled Recovery Test will be rescheduled as soon as possible.

1.4.3. Test Services — Features

Sungard AS will provide certain Resources to Customer for Customer to "Test for the number of Test Periods stated in the Order.

Each test period equals 48 hours of consecutive Test time per contract year on a non-cumulative basis ("Test Period").

Customer will comply with Sungard AS' Test Scheduling & Cancellation Policy. All Tests are subject to immediate cancellation by Sungard AS if and when any other customer declares an Event and requests use of the Resources being tested. Any such cancelled Test will be rescheduled as soon as possible.

1.5. Cloud Repository Availability

1.5.1. Agreement

The Cloud Repository shall be operational and available for Customer data transmission 99.9% of the time. Availability will be measured on a monthly basis using internal monitoring software.

1.5.2. Remedy

If Sungard AS fails to meet the Cloud Repository Availability SLA, Customer is entitled to a credit equal to 10% of the Order's monthly fee for the month in which the failure occurs.

1.6. Cloud Backup and Recovery — Infrastructure SLA

1.6.1. Agreement

For Recovered Servers selected in the Order, at time of an Event, Sungard AS will provide the Resources, provided that this SLA does not amend, modify or otherwise alter the Multiple Activation provisions concerning Resource use and allocation.

Infrastructure (Hypervisor Level)	Period of Time	Uptime Availability
VM Availability	At Time of Event	99.95% Uptime at the Hypervisor Level
Storage Services Availability	At Time of Event	99.99%

The above SLAs apply only following the completion of a successful user acceptance test. Such a test is to be completed after the successful implementation of the Services and completion of a test post-implementation. The above SLA will not apply at the time of a Recovery Test.

1.6.2. Remedy

If Sungard AS fails to meet the Cloud Backup and Recovery — Infrastructure SLA at the hypervisor level at time of an Event, Customer is entitled to a credit equal to 15% of the monthly fee for the Cloud Backup and Recovery Service for the month in which the failure(s) occur(s), regardless of how many failures occur in the said month. All Cloud Backup and Recovery — Infrastructure SLA failures within a calendar month will count as a single SLA violation for purposes of calculating the termination right described in the General Service Terms.

1.7. Cloud Backup and Recovery — Recovery Time Objective (RTO) SLO

1.7.1. Recovery Time Objective SLO

This SLO covers the recovery of the Protected Servers and the associated OS and data.

Sungard AS will provide support and assistance for a successful recovery, except if Customer:

(a) Fails to correctly transfer its data
(b) Uses software and hardware not supported by Sungard AS
(c) Uses any backup or deduplication technology that requires restoration in conjunction with storage replication
(d) Customer makes changes to the recovery plan that exceed the contracted resources

Number of Virtual Protected Servers	Recovery Time Objective SLO
First 100 servers recovered	8 hours
Every additional 100 servers recovered	4 hours

2. GENERAL SERVICE TERMS

These Services are also subject to the General Service Terms at https://www.sungardas.com/hubfs/_multimedia/document-file/sungardas-general-service-terms.pdf.