SPAIN MANAGED SERVICES
CLOUD PROTECTION POLICY

6 November 2019

This Spain Managed Services – Cloud Protection Policy ("Policy") supplements and sets forth additional terms and conditions governing the provision of the Cloud Protection Service, as specified in the applicable Order. This Policy shall form part of the terms and conditions of the Order and the Master Country Agreement or other similar agreement between the Parties ("Agreement").

1. Service Description

1.1 Definitions

Capitalized words used in this Policy will have the meaning ascribed to them herein, but if not defined in this Policy, shall have the meaning ascribed to them in the Agreement.

"**Application Integration**" means Standard Application Integration or Public Cloud Applications Integration, which are features of the Cloud Protection Service, as described further in this Policy.

"**Backup**" means as the context requires either a First Backup, a Full Weekly Backup or an Incremental Daily Backup.

"**Backup Data**" means the data from a specified and agreed part of a Customer's Platform, in the form it is in when retrieved in a Backup.

"**Backup Platform**" means Equinix's backup platform.

"**Cloud Protection Service**" means the Cloud Protection Service, as described further in this Policy.

"**CP Fees**" means the Fees payable for the applicable calendar month for the affected Cloud Protection Service.

"**Customer's Platform(s)**" means Customer's virtual environment(s), provided by a public cloud provider's public cloud service.

"**First Backup**" means the first copy of all Backup Data.

"**Full Weekly Backup**" means:

a) except as set out in paragraph (b) below, a consolidation of the First Backup or most recent Full Weekly Backup (as applicable) with all the Incremental Daily Backups taken since the later of the First Backup or most recent Full Weekly Backup (as applicable) performed once per week; or

b) for third party application data and databases forming part of the Backup Data when Application Integration is purchased by Customer, a full copy of such parts of the Backup Data performed once per week.

"**Incremental Daily Backup**" means a copy of the incremental changes to the most recent Backup performed once per day.

"**Media**" means the virtual machine in the Customer's Platform(s) with the capability to index and store the Backup Data.

"**Proxy**" means the virtual machine in the Customer's Platform(s) with the capability to communicate between the Customer's Platform(s) and the Backup Platform, and facilitate communication between them of the catalogue information regarding the Backup Data.

"**Storage Account**" means logical account within the Customer's Platform(s) where the Backup is stored (object storage usually).

1.2 Set Up

In setting up the Cloud Protection Service, Equinix will consult with the Customer to ascertain backup configuration information.

Equinix will install and configure or enable the Customer to install and configure:

A. backup software on the Customer's Platform(s);

B. where agreed in an Order, a connection from Customer's Platform(s) to the Backup Platform;

C. where agreed in an Order for an additional Fee, Media and Proxy installation on the Customer's Platform(s), and Equinix will establish the sizing of the Media and Proxy based on the predicted volume of the Backup Data, and the recommended configuration per size detailed in Appendix 2 to this Policy; and

D. if necessary in Equinix's reasonable discretion, management connections to Customer's Platform(s) (Media and Proxy) from the Backup Platform.

Customer acknowledges that the Backup Platform is hosted in a public cloud environment, and if necessary consents to Equinix subcontracting relevant obligations to the relevant public cloud vendor.

1.3 Cloud Protection Services

The Cloud Protection Service provides a backup services for a public multi-cloud environments (see Appendix 1 for the public cloud providers and services supported). Backup Data is managed and indexed by the Backup Platform, but stored on the Storage Account to ensure the Backup remains on Customer's Platform(s) and optimises data transfer. The Cloud Protection Service will, via the Cloud Protection Platform and at the times agreed with the Customer, complete:

A. a First Full Backup, and thereafter a Full Weekly Backup; and

B. an Incremental Daily Backup;

with the following features as indicated in the applicable Order:

FEATURE	DESCRIPTION	INCLUDED / OPTIONAL
Full Weekly Backups	After the First Backup, the Full Weekly Backup consolidates the last Full Weekly Backup with subsequent Incremental Daily Backups.	Included
Deduplication at source	The Backup Platform will identify blocks of Backup Data that are already in a Backup, and will not send such data to the Storage Account as part of a Full Weekly Backup or an Incremental Daily Backup.	Included
Backup of virtual machines and FileSystems	The Backup Platform can support copying Backup Data from public cloud virtual machines at virtual machine level or filesystem level.	Included
Standard Application Integration	The Backup Platform can integrate with different commercial standard applications installed on public cloud virtual machines and perform backups using native tools.	Optional
Public Cloud Applications Integration	The Backup Platform can integrate with different public cloud applications supported (see Appendix 1)	Optional, but is Included when Backup Data is taken from any of the public cloud applications supported in Appendix 1, except for Cloud Virtualization
Encrypted/Encoded Backup	Backups can be independently encrypted at source, during the communication process and at destination with an encryption algorithm managed by the Backup Platform	Optional
Replication in an IBX Center (MD2, MD1, BA1)	A second copy of the Full Weekly Backup is stored on a separate storage location in an IBX Center.	Optional

Once a Backup is complete, the Storage Account will retain the Backup Data for the applicable retention period, depending upon the retention standard specified in the Order, which are described below:

RETENTION PRODUCT	RETENTION PERIOD FROM DATE OF RELEVANT BACKUP	DESCRIPTION
BASIC RETENTION	One week	Each Full Weekly Backup and Incremental Daily Backup will be retained for the Retention Period
STANDARD RETENTION	One month	Each Incremental Daily Backup will be retained for the Retention Period
	One month	The First Backup and thereafter each Full Weekly Backup will be retained for the Retention Period
EXTENDED RETENTION	One month	Each Incremental Daily Backup will be retained for the Retention Period
	One month	The First Backup and thereafter each Full Weekly Backup will be retained for the Retention Period
	One year	One Full Weekly Backup per month will be retained for the Retention Period
	Five years	One Full Weekly Backup per year will be retained for the Retention Period

Equinix will provide the Customer with the Backup status via its online customer portal. A report with such information via email is available as an option.

2. Customer Responsibilities

The provision of the Cloud Protection Service is dependent on the following Customer responsibilities and if the Customer fails to perform or fulfil the Customer responsibilities, Equinix will not be obliged to provide the Cloud Protection Service and may charge additional non-recurring Fees that are caused by or arise from such failure to perform or fulfil the Customer responsibilities:

A. Customer must, or must authorise and provide necessary support for Equinix to, create and maintain for the full Term a connection between the Customer's Platform(s) and the Backup Platform, and

B. Customer must determine the specification of and maintain (including paying the relevant cloud provider for): (i) the Customer's Platform(s); (ii) the Media and Proxy on the Customer's Platform(s), (iii) the Storage Account on the Customer's Platform(s), and (iv) any inter-cloud connection methods between Customer's Platforms.

C. Customer must provide all necessary information to enable Equinix to set up any required connections between Customer's Platform(s) and the Backup Platform and ascertain any other backup configuration information.

D. Customer must: (i) ensure Customer's Platform(s) remains functional and compatible with the original settings agreed during set up, (ii) maintain and not amend Customer's Platform(s) settings or configuration, or operating system platform or configuration, except with Equinix's prior consultation, and (iii) maintain and not amend the configuration of any relevant software installed on Customer's Platform(s).

3. Charging Methodology

Where a defined term in this Charging Methodology is not defined in this Policy, its meaning shall be as described in the Support Services Policy.

The Unit of Measure (UoM) used to determine the volume consumed or available for consumption of the Cloud Protection Service for the purpose of the different Fees payable by Customer, is the volume of terabytes (Protected TB) that is available to be consumed or actually consumed (as applicable) by Customer as a Backup on the Storage Account.

For these purposes, Overage Charges and Pay As You Go Charges shall be calculated using the peak volume of the UoM Protected TB in the Full Weekly Backup for Service Period.

The Fees for the Cloud Protection Service will accrue from the Effective Date. For the avoidance of doubt, the MRC, Pay-As-You-Go Charges and/or Overage Charges may be invoiced earlier than the Setup Fee where for reasons not attributable to Equinix, some of the Customer's Platform(s) is not yet ready to be included in a Backup.

4. Service Level Agreement

The purpose of this Service Level Agreement ("**SLA**") is to define the measurable performance levels for the Cloud Protection Service and specify remedies available to Customer if Equinix fails to achieve these levels. The service credits listed in the tables below are the sole and exclusive remedy for any failure to meet the service level thresholds stated herein.

Backup Platform at 99.5+% availability. This is met by achieving less than two hundred and nineteen (219) minutes of Unavailability of the Backup Platform over a calendar month period ("**Backup Platform SLA Threshold**"). For the purposes of this paragraph and subject to the last paragraph of this section, the Backup Platform is considered "**Unavailable**" when a failure in the Backup Platform means that it is unable to establish and maintain a communication to the Customer's Platform(s) due to a failure in the Backup Platform. The period of Unavailability is measured from Customer's notification to Equinix of the incident to the time the Unavailability has been remedied as confirmed by Equinix. Subject to the last paragraph of this section, if Unavailability exceeds the Backup Platform SLA Threshold, Customer will be entitled to a credit equal to 1/30th of the CP Fees. Further, Customer will be entitled to an additional credit equal to 1/30th of the CP Fees for every full hour of Unavailability beyond the Backup Platform SLA Threshold.

Restoration Commencement Time. Following the submission of Customer's request on Equinix's support systems, Equinix will commence the restoration of the requested Backup to the Storage Account within the applicable Restoration Commencement Target. For each such request, the "**Restoration Commencement Time**" is measured during the applicable Request Window from the submission of Customer's complete request on Equinix's support systems for the restoration of a Backup and up to the initiation of the restoration of such Backup on the Backup Platform (each a "**Valid Request**"). After receiving a Valid Request, Equinix reserves the right to modify the Urgency allocated to the Valid Request based on the description below.

SERVICE LEVEL NAME	METRIC	URGENCY	RESTORATION COMMENCEMENT TARGET	REQUEST WINDOWS	RCT THRESHOLD
Restoration Commencement Time	Subject to the last paragraph of this section, this metric is calculated as the total number of Valid Requests in a calendar month where the Restoration Commencement Time is within the applicable Restoration Commencement Target, divided by the total number of Valid Requests in such calendar month, with the results expressed as a percentage to two (2) decimal places.	High	<4 hours	24x7	95.00%
		Moderate	<6 hours	8am to 5pm on business days in Madrid	
		Low	<8 hours	8am to 5pm on business days in Madrid	

URGENCY	DESCRIPTION
High	A request that must be prioritized as restoration is essential to avoid putting at risk the Customer's business, its services to its customers or its projects
Moderate	A request that can be responded to sequentially, as a delay in restoration will not put at risk the Customer's business, its services to its customers or its projects
Low	A request that should not be prioritized, as a delay in restoration will not put at risk the Customer's business, its services to its customers or its projects

Subject to the last paragraph of this section:

(A) if there are twenty (20) or more Valid Requests in a calendar month and the RCT Threshold is not met or exceeded, then Customer will be entitled to a credit equal to 1/30th of the CP Fees; or

(B) if there are less than twenty (20) Valid Requests in a calendar month and there are two (2) or more Valid Requests in a calendar month that each had a Restoration Commencement Time that was not within the applicable Restoration Commencement Target, then Customer will be entitled to a credit equal to 1/30th of the CP Fees.

General. In any calendar month, the maximum credit to which Customer will be entitled will not exceed the CP Fees payable for the affected Cloud Protection Service in such calendar month. Customer must request a credit within thirty (30) days of the date of its occurrence by contacting the Equinix Service Desk, so Equinix may investigate and isolate the cause of the failure. All periods of Unavailability or failure to meet the applicable Restoration Commencement Time must be verified by Equinix. Approved credits will be applied by Equinix to the invoice for the month following the month in which the credit was approved. Notwithstanding anything to the contrary, the SLAs will not apply and Equinix will have no liability if the Unavailability or failure to meet the Restoration Commencement Time: (a) is caused by circumstances beyond Equinix's reasonable control; (b) is caused by Customer's act or omission; (c) is caused by Customer's Platform(s), software or connectivity on or between Customer's Platform(s) and the Backup Platform; (d) is caused by execution of any scripts on Customer's Platform(s); (e) is caused by functional failures as a result of third-party applications running on Customer's Platform(s); (f) that occurs during a scheduled maintenance window; or (g) is caused by a failure in the public cloud vendor platform on which the Backup Platform is hosted. Equinix will use reasonable efforts to notify Customer at least fourteen (14) days prior to any regularly scheduled maintenance and as soon as practicable before any emergency maintenance. Equinix will use commercially reasonable efforts to minimize disruption to Customer's Services when performing scheduled maintenance.

5. Miscellaneous

Equinix's customer support for the Services described in this Policy are outlined in the Support Services Policy available www.equinix.com/resources/product-documents/. This Policy and the Order, together with the Agreement, represents the complete agreement and understanding of the Parties with respect to the subject matter herein and in the Order, and supersedes any other agreement or understanding, written or oral.

Appendix 1: Services Supported

Cloud Protection Service supports the following public cloud services but excludes any standard backup software agent supported in the Spain Managed Services - Smart Backup Policy (listed below):

	AWS	MS AZURE	GOOGLE CLOUD	ORACLE CLOUD	ALIBABA	OTHERS
CLOUD VIRTUALIZATION	AWS Instances	Azure VMs	Google Cloud Instances	Oracle Cloud Instances		Docker
STORAGE	Amazon FSx For Windows File Server AWS EFS Amazon S3	Azure Blob Storage	Google Cloud Storage	Oracle Storage Cloud Services		
DATABASE SERVICES	Amazon RDS	Azure Database	Google Cloud Database		Alibaba RDS	
CLOUD APPS		Azure Stack	Gmail And Google Drive	Oracle PaaS		OpenStack Swift
BIG DATA APPS	Apache Cassandra, Greenplum and MongoDB databases					

Standard backup software agents supported in the Spain Managed Services - Smart Backup Policy:

- Active Directory
- DB2
- DB2 MultiNode
- Documentum
- GlusterFS
- Hadoop (HDFS)
- Image Level
- Informix
- IBM Notes or IBM Domino
- IBM i File System Agent
- IBM i File System Agent with Commvault VTL
- IBM Spectrum Scale (GPFS)
- Lustre File System
- Macintosh File System
- Microsoft SharePoint Server Agent
- Microsoft SQL
- Microsoft Windows
- MySQL
- NDMP
- Network Share
- Nutanix Files
- Open Enterprise Server (OES)
- Oracle
- Oracle RAC
- OpenVMS
- PostgreSQL
- SAP
- Sybase
- UNIX/Linux File Systems
- Online Help

Appendix 2: Media Agent and Proxy recommended sizing

Recommended Media agent sizing is based on the predicted volume of the Backup Data (AWS example set out below):

AWS Mediaagent Specifications

EXTRA SMALL	SMALL	MEDIUM	LARGE	EXTRA LARGE
60 TB BET	120 TB BET	240 TB BET	600 TB BET	800 TB BET
Up to 60 TB estimated back-end data	Up to 120 TB estimated back-end data	Up to 240 TB estimated back-end data	Up to 600 TB estimated back-end data	Up to 800 TB estimated back-end data
m5.xlarge EC2 instance (EBS-optimized, 4 vCPU, 16GB RAM) or m4.xlarge EC2 instance (EBS-optimized, 4 vCPU, 16 GB RAM)	m5.2xlarge EC2 instance (EBS-optimized, 8 vCPU, 32 GB RAM) or m4.2xlarge EC2 instance (EBS-optimized, 8 vCPU, 32 GB RAM)	m5.2xlarge EC2 instance (EBS-optimized, 8 vCPU 32 GB RAM) or m4.2xlarge EC2 instance (EBS-optimized, 8 v CPU, 32 GB RAM)	m5.4xlarge EC2 instance (EBS-optimized, 16 vCPU, 64 GB RAM) or m4.4xlarge EC2 instance (EBS-optimized, 16 vCPU, 64 GB RAM)	m5.12xlarge EC2 instance (EBS-optimized), 48 vCPU, 192 GB RAM) or m4.10xlarge EC2 instance (EBS-optimized, 40 vCPU, 160 GB RAM)
1x 200 GB EBS General Purpose SSD (gp2) volume for DDB	1x 400 GB EBS General Purpose SSD (gp2) volume for DDB	1x 600 GB EBS General Purpose SSD (gp2) volume for DDB	1x 1.2 TB EBS Provisioned IOPS SSD (io1) volume for DDB @ 15,000 IOPS	1x 2 TB EBS Provisioned IOPS SSD (io1) volume for DDB @ 20,000 IOPS
1x 400 GB EBS General Purpose SSD (gp2) volume for index cache	1x 400 GB EBS General Purpose SSD (gp2) volume for index cache	1x 1 TB EBS General Purpose SSD (gp2) volume for index cache	1x 1 TB EBS General Purpose SSD (gp2) volume for index cache	1x 2 TB EBS General Purpose SSD (gp2) volume for index cache
Linux or Windows Server 2012 R2 or Windows Server 2016 (Commvault V11 SP7+)	Linux or Windows Server 2012 R2 or Windows Server 2016 (Commvault V11 SP7+)	Linux or Windows Server 2012 R2 or Windows Server 2016 (Commvault V11 SP7+)	Linux or Windows Server 2012 R2 or Windows Server 2016 (Commvault V11 SP7+)	Linux or Windows Server 2012 R2 or Windows Server 2016 (Commvault V11 SP7+)

Recommended Proxy sizing will be stated in the applicable Order, and Equinix would otherwise determined depending on the size of the Media and estimated volume of the Backup Data.