Enterprise Claro Cloud Technical and Service Management Terms and Conditions

1. INTRODUCTION

The Enterprise Claro Cloud (the "Service") is a next-generation cloud platform based on VMware technology for hosting customer business applications on a virtualized, shared infrastructure with flexible, on-demand computing capabilities and a pay-as-you-go pricing model.

The Services are deployed in a Virtual Data Center (Org-VDC) in an isolated and secure manner with the possibility to connect to other infrastructures via the Internet, virtual private networks (VPN), or MPLS-based enterprise data networks. Services can be configured through a Self-Service Portal or via programmable interfaces (APIs).

Enterprise Claro Cloud offers the following features:

a. Compute: Provision of Org-VDC, Virtual Machines, and Kubernetes Cluster with variable processing (vCPU) and memory (RAM) capabilities.

b. Storage: Provision of solid-state disk (SSD) volumes for dedicated virtual machines and on a shared basis.

c. Network and Security: Virtual network services such as firewalls, load balancers, routing, NAT, public IP addressing, secure IP-VPN connections, and MPLS data networks.

d. Backup and Replication — Separate backup infrastructure for backing up and recovering Kubernetes virtual machines and clusters. Configuration of replication between different computing regions.

e. Application Catalog: Access to a curated catalog of open-source applications from a curated catalog of applications for easy deployment to virtual machines, containers, and Kubernetes.

2. SERVICES PROVIDED BY ENTERPRISE CLARO CLOUD

2.1 Computing Regions

The Enterprise Claro Cloud Service will be provided in 10 data centers throughout the United States and Latin America.

Available Enterprise Claro Cloud Regions:

Country	City
Argentina	Buenos Aires
Brazil	Sao Paulo
Chile	Santiago de Chile
Colombia	Bogotá
Ecuador	Guayaquil
United States	Miami
Guatemala	Guatemala (availability TBD)
Peru	Lima (availability TBD)
Puerto Rico	San Juan (availability TBD)
Dominican Republic	Santo Domingo

2.2 Service provisioning

The initial contracting of the Service is performed by the CUSTOMER through the Enterprise Claro Cloud Self-Service Portal.

Following execution of the Claro Enterprise Solutions MSA, Service Annex, and Order Form, the Customer will receive a welcome email with its administrator username, instructions for setting its password, and the URL (https://sso.clarocloud.com) of the Enterprise Claro Cloud Self-Service Portal for configuring the Services and registering additional Users. The Claro Enterprise Solutions service delivery team will provision the Customer initially; all subsequent provisioning will be conducted by the Customer through the Enterprise Claro Cloud Self-Service portal.

MPLS Virtual Private Data Network Service for Virtual Data Center Access (Org-VDC) is contracted separately.

2.3 Connectivity Options

There are two types of connectivity options for Virtual Data Centers (Org-VDC):

a. Internet: Access to Self-Service Portal, APIs, and Services via the Internet.
b. Hybrid (Internet + MPLS): Access to the Self-Service Portal, APIs, and Services over the Internet, plus a network interface to interconnect the Customer's Virtual Data Center to MPLS virtual private data networks.

2.4 Virtual Organization

Each customer has a virtual organization in the Enterprise Claro Cloud environment, which allows the secure separation of services. The organization includes at least one Virtual Data Center (Org-VDC) and one T1-Gateway.

2.5 Virtual Data Center (Org-VDC)

The Virtual Data Center (Org-VDC) is a group of resources that defines the usable cloud capacity in vCPU, RAM, and storage for services within a specific virtual organization. The Customer can select the computing region and resource allocation model for its Virtual Data Center.

a. On-Demand: In this allocation model, computing resources such as vCPU, RAM, and storage do not have a limit and are billed monthly according to their consumption. The limit is set by the available capacity of the underlying cloud infrastructure in each Compute Region.
b. Resource Pool: In this allocation model, in the Enterprise Claro Cloud Self-Service Portal, the CUSTOMER may purchase, increase, or decrease the number of vCPUs, RAM, and storage required for each Virtual Data Center. The capacity of each Virtual Data Center under the Resource Pool type is limited to the number of resources contracted by the Customer.

2.6 Storage (Premium SSD Disk)

Premium SSD data storage is hosted in the same Region where the computing resources of each Virtual Data Center (Org-VDC) contracted by the Customer are located.

The entire storage infrastructure is based on next-generation high-performance solid-state disks (SSDs) configured with a RAID 6 protection policy. Storage is also considered as occupied space, the GiB allocated by the SWAP memory of each virtual machine.

The storage performance granted per gigabyte (GB) is equivalent to 1.5 IOPS per GB of allocated storage.

2.7 Self-Service Portal

The Self-Service Portal https://sso.clarocloud.com is a web application that the Customer can only access via HTTPS by entering a valid username, password, and a two-factor authentication code through the VMware Verify application. The Self-Service Portal allows customers to manage virtual

services using remote access. The VMware manufacturer's user guide is available in the Help section of the Self-Service Portal.

The Self-Service Portal supports the following languages: English, Spanish, and Portuguese. The portal user interface adopts the language configured in the web browser of the Customer's device.

2.8 Enterprise Claro Cloud APIs

All functions available through the Self-Service Portal can be called through a REST-based API. The API documentation is available in the Help section of the Self-Service Portal.

2.9 User and Role Management

The Customer can create additional users and assign them predefined roles with different authorization levels using the Organization Administrator account.

Role	Description
Account Administrator	Allows the user to purchase, modify, and cancel virtual Data Center subscriptions in on-demand mode and resource pool. This role provides access to the Enterprise Claro Cloud control panel only.
Organization Administrator	Allows users to purchase additional services available through the Self-Service Portal, such as Edge Gateway, load balancers, and public IP addresses. A user can create additional users and assign them different default roles. The user can perform all configuration and administration tasks available in the Self-Service Portal, such as creating, modifying, and deleting virtual machines and networks within an Org-VDC. Access to administrative information and consumption reports.
Compute Administrator	Allows creation, modification, and deletion of virtual machines, applications, and management of deployed computing resources through the Self-Service Portal and API.
Network Administrator	Allows creation, modification, and deletion of networks, firewall rules, NAT configurations, and public IPs within Edge instances through the Self-Service Portal and API.

Technical Administrator	Allows users to create, edit, and delete networks, firewall rules, virtual machines, applications, and manage deployed resources through the Self-Service Portal and API. User cannot: • Purchase additional services within the Self-Service Portal. • Edit administrative information. • Modify computing resource limits. • Change roles or add other users.
Staff-Read Only	Allows query-only access to review instance, network configuration parameters, and monitor the status of different tasks and objects. Users cannot generate new instances, delete or change instance configuration settings, or perform administrative tasks.

2.10 Virtual Applications (vApp)

A group of virtual machines (VMs) facilitates the work and management of complex applications.

2.11 Console Access to Virtual Machines

Access the graphical user interface (GUI) of virtual machines directly from the Self-Service Portal via the Access Console.

2.12 Remote Console Access to Virtual Machines

The Customer must install an add-on depending on the operating system/browser installed locally. The add-on is available within the Self-Service Portal and at the URL (www.clarocloud.com/portal/downloads).

2.13 Virtual Networks

The Customer can create logically isolated network segments according to its needs and be assigned to different virtual machines to communicate with them. There are diverse types of virtual networks:

a. Isolated within a VDC: Allows communication between virtual machines belonging to the same Virtual Data Center.
b. Separated between different VDCs: Allows communication between other Virtual Data Center VMs but always belonging to the same computing region.
c. Routed: Allows communication between virtual machines in a Virtual Data Center to external LAN networks within the Data Center or WAN over the Internet or MPLS.

d. Micro segmentation allows the customer to divide the Virtual Data Center network segments into different security segments with varying security policies and great granularity controls.

2.14 Virtual Firewall

Firewall functions based on an instance called T1 Edge Gateway. The initial configuration of the firewall blocks inbound and outbound traffic to the Virtual Data Center. The Customer's responsibility is to create the necessary firewall rules to allow the desired traffic to the Virtual Data Center.

T1 Edge Gateway also allows customers to apply routing, NAT, and port filtering configurations. Any external network traffic (e.g., private network connections, secure Internet access)

2.15 Load Balancer (NSX Advanced Load Balancer)

Allow customers to configure VMware technology-based traffic balancing, web application firewall, and container ingress functions for applications within Virtual Data Centers.

2.16 Catalogs and Templates

The Customer will have access to a catalog with predefined templates. A template is a pre-designed master configuration used to create virtual machines automated through the Self-Service Portal. The Customer can create a catalog and upload its templates or create new templates from existing virtual machines.

For all virtual machines, the Customer is given administrative rights (root), auto-generated access passwords, and can be viewed and modified in the Self-Service Portal, in the OS properties section.

a. Predefined General-Purpose templates: The computing power of these virtual machines is backed by scalable Intel® Xeon® Gold processors.

Templates	vCPU	RAM (GB)
gp.xsmall-01	1	1
gp.small-01	2	4
gp.small-02	2	8
gp.medium-01	4	8
gp.medium-02	4	16
gp.medium-03	8	16

gp.medium-04	8	32
gp.large-01	16	32
gp.large-02	16	64
gp.xlarge-01	32	96
gp.xlarge-02	32	128

b. Custom Template: The CUSTOMER can allocate any combination of a number of vCPUs and GB of RAM.

Resource	Lower limit	Upper Limit
vCPU	1	256
RAM memory (GB)	1	2048

c. Block storage with SSD Premium performance policy is allocated independently to each Virtual Machine according to the CUSTOMER's needs.

Resource	Limit
SSD block storage (GB)	10 – 10,000

2.17 Native Kubernetes Clusters

Creation of Native Kubernetes clusters based on virtual machines, adapting computing resources to the needs of each CUSTOMER.

Operating Systems	Ubuntu / Photon
Number of Master Nodes	One per Cluster
Number of Worker Nodes	N per Cluster
Virtual Machine Size for Worker No les	
vCPU (min/max.)	1 / 256 vCPU
GB RAM memory (min/max.)	1 / 2048 GB

Amount of Master Node: One (1) per cluster provisioned via the control panel; multiple modes available via APIs.

The Master Node within the Kubernetes cluster is provisioned by default every time a new cluster is contracted. There can only be a maximum of one Master node per cluster.

Storage is allocated independently to each node according to the CUSTOMER's needs.

Resource	Limit
SSD block storage (GB)	10 – 10,000

2.18 Multi-region High Availability Zone and Disaster Recovery

To implement high-availability zones by configuring replicated services between virtual data centers located in different computing regions, the CUSTOMER must contract at least two Org-VDCs in different computing regions (location) of Enterprise Claro Cloud, distribute the virtual machines corresponding to an application across the two locations, and configure them using application specific synchronization and disaster recovery mechanisms. The following considerations apply:

a. The CUSTOMER's responsibility is to ensure that sufficient computing resources have been contracted and/or configured in the non-affected region.
b. Enterprise Claro Cloud aims to consider the CUSTOMER's requirements and restore time to a minimum.
c. To use this functionality, the CUSTOMER must request activation of the service through Enterprise Claro Cloud Support.

2.19 VMS/vApps Snapshots

Snapshot functionality to create an online copy of a virtual machine or vApp at a time. Customer can only maintain a single Snapshot at a time for a virtual machine or vApp. The Snapshot is not a substitute for a backup, so it is recommended that the Snapshot duration does not exceed 24 hours.

2.20 Backup as a Service (BaaS) (Beta version)

The backup service allows customers to create single or rule-based backups and restores with different retention policies through the Self-Service Portal and through the Agent (Additional software). Backup profiles are predefined and not modifiable. They differ in frequency, type of backup, and data retention period.

Plan	Frequency	Backup Strategy Type	Retention Period	Time to execution
A	Daily	1st Full + incremental	7 days	10:00 pm
B	Weekly	1st Full + incremental	7 days	Viernes, 10:00 pm
C	Daily	1st Full + incremental	30 days	10:00 pm
D	Monthly	1st Full + incremental	1 year	10:00 pm
E	Monthly	1st Full + incremental	10 years	10:00 pm
NA	On demand	Full/incremental/synthetic	On demand	On demand

Backups are stored on dedicated, independent infrastructure located in the same computing region that hosts the respective virtual machines. Backup and restoration tasks can only be executed within the same computing region of Enterprise Claro Cloud Empresarial.

You can restore virtual instances through two mechanisms:

Restauration	Description
In place	Restores data directly on the existing virtual instance.
Out of place	Creates a new virtual instance within the Virtual Data Center with characteristics different from the source machine.

Regions with the Backup service:

- Argentina
- Brazil
- Chile
- Colombia
- Ecuador
- Dominican Republic
- USA

Considerations:

- If a customer deletes a virtual machine where a backup was configured, a charge will be applied as long as the backup remains active, based on the average monthly usage.

Therefore, it is the customer's responsibility to delete backups of virtual machines they no longer need.

- Upon full cancellation of a subscription that had a configured backup, the backup copies will be removed from the Backup platform, and there will be no way to restore them.
- There is no penalty for canceling a backup schedule.
- Backups are unavailable on on-premises servers.
- There is no storage limit for backups, but if copies are retained, storage usage will be billed accordingly.
- Claro Enterprise Solutions' monitoring is focused on the platform itself, not on individual CUSTOMER configurations or CUSTOMER-specific errors.

2.21 vCloud Availability

Allows customers to configure continuous replications of vApps or VMs through the Self-Service Portal. Workloads can be migrated or protected. Migration is a one-time action with a 24-hour recovery point objective (RPO). Protection continuously replicates the workload, and the Customer can select from predefined RPO values and, optionally, choose a predefined retention policy for spot instances. Workloads can be migrated or secured in the following scenarios:

a. From VMware vCenter servers on customer premises to Enterprise Claro Cloud
b. From one Org-VDC to another Org-VDC within Enterprise Claro Cloud in different regions

2.22 Performance Adjustments in Favor of the CUSTOMER

Claro Enterprise Solutions reserves the right to make unilateral changes to expand the Service and modify charges related to the CUSTOMER. The CUSTOMER accepts such adjustments.
Claro Enterprise Solutions will notify the CUSTOMER of any such changes.

2.23 Resource Limit Adjustments.

Claro Enterprise Solutions reserves the right to make unilateral changes to establish limits on the total number of virtual machines and computing resources that the CUSTOMER may contract within a virtual organization or Virtual Data Center (Org-VDC). The CUSTOMER accepts such adjustments. Claro Enterprise Solutions will notify the CUSTOMER of any such changes.

2.24 Horizontal Auto-Scaling

The CUSTOMER may enable horizontal auto-scaling from their control panel, allowing additional virtual machines to be added to their organization based on the utilization of their computing resources, to maintain the operational stability of their applications.

2.25 Internet access

The Customer can activate incoming and outgoing data traffic to the Internet to its virtual machines within its VDC; traffic is routed directly to the Internet through the Customer's T1 Edge Gateway.

The T1 Edge Gateway at the edge of the Virtual Data Center allows the Customer to route IP traffic to multiple virtual machines and deploy multiple expanded network services. This includes independent management of the virtual firewall, NAT configuration, and load balancer configuration for the Virtual Data Center network.

2.26 Supported Ports and Protocols

Secure Internet access for inbound and outbound data traffic is blocked as the initial configuration policy of the virtual firewall. The customer must configure rules on the virtual firewall of the T1 Edge Gateway that allow it to accept traffic based on the desired communication protocols and ports.

2.27 Security and Network Service

Claro Enterprise Solutions provides a virtual firewall associated with the T1 Edge Gateway, in which the Internet connection is terminated. The Customer does the configuration of the virtual firewall through the Self-Service Portal.

2.28 Internet Bandwidth

Claro Enterprise Solutions does not limit Internet bandwidth per customer. Rather, Internet bandwidth is limited by the underlying network infrastructure configured in high availability. Claro Enterprise Solutions reserves the right to apply fair use policies or data transfer controls, including partial or total blocks if any abuse of resources is detected.

2.29 MPLS Direct Connection

For the hybrid T1 Edge Gateway type, Claro Enterprise Solutions supports the connection of Data Centers and other remote Customer sites to the Enterprise Claro Cloud platform through the MPLS Virtual Private Network service. Claro Enterprise Solutions provides a termination point in the respective Virtual Data Center to connect via MPLS. The customer must contract the MPLS Virtual Private Network service.

2.30 Layer 2 VPN

Within the T1 Edge Gateway, it is possible to configure a point-to-point Layer 2 VPN through the Self-Service Portal using the Internet connection.

2.31 Point-to-Point VPN

Within the T1 Edge Gateway, it is possible to configure a point-to-point VPN through the Self-Service Portal using Internet access.

2.32 Data Transfer Input and Output (I/O)

Claro Enterprise Solutions does not limit the transfer of data to the Virtual Data Center, and the limit is based on the physical capacity of the link in the data center where the infrastructure is hosted.

2.33 T1 Edge Gateway

A virtual edge instance that allows the customer to manage the virtual firewall and internal networks of a Virtual Data Center.

2.34 Distributed Virtual Firewall (East-West)

Through the T1 Edge Gateway, the customer can configure policy-based firewall rules to microsegment traffic within the internal network of the Virtual Data Center, protecting traffic between virtual machines on that same network.

2.35 Public IPv4 IP Addresses

The first Public IP address is assigned and configured when the first Virtual Data Center (Org-VDC) is created in each Region. The Customer may purchase additional public IPs at a cost. Through the Self-service Portal, the CUSTOMER routes TCP ports from an external IP to different virtual machines, reducing the number of public IPs required and increasing flexibility. The Customer can do so through the Self-Service Portal. Only public IP addresses used will be billed.

2.36 Operating Systems

Claro Enterprise Solutions operates updated versions of Windows Server, RedHat Enterprise Linux, and SUSE Enterprise Linux operating systems and publishes them in the public catalog. The images provided are regularly updated according to the lifecycle of new versions and vulnerabilities issued by their respective manufacturers.

Periodically, each operating system manufacturer announces an End of Support (EOS) or End of Life (EOL) date for each version of their operating systems used in Enterprise Claro Cloud. For operating systems that reach their EOS or EOL date, the following will occur:

- Claro Enterprise Solutions will no longer be able to provide support or assistance for provisioned virtual.
  machines.
- Claro Enterprise Solutions will no longer have access to updates.

- Claro Enterprise Solutions will no longer have access to security patches.
- Operating system images will be removed from the public catalog and moved to a legacy catalog for a defined period.

If the CUSTOMER runs virtual machines based on any of these operating system images that have reached their EOS or EOL date, the CUSTOMER must consider the following:

- Virtual machines with operating systems provisioned after the EOS or EOL date will continue to operate, and billing will remain unchanged.
- Some functionalities or performance may not operate as expected when using an operating system past its EOS or EOL date.
- Virtual machines with operating systems provisioned after the EOS or EOL date will remain vulnerable to potential security threats.
- Claro Enterprise Solutions will no longer be able to provide any assistance, updates, or security patches. The CUSTOMER will assume responsibility for installing and testing any updates provided by a manufacturer or third party.

It is recommended that the CUSTOMER replace or upgrade any virtual machine running on Enterprise Claro Cloud within no more than three (3) months after the EOS or EOL date.

a. Available Operating System Versions

Operating System	**End of Support Claro Enterprise Solutions (EOS)**	**End of Life (EOL)**	**Catalog**
Microsoft Windows Server 2012 Standard R2	Oct-18	Oct-23	No Available
Microsoft Windows Server 2016 Standard R2	Ene-22	Ene-27	Legacy
Microsoft Windows Server 2019	Ene-24	Ene-29	Legacy
Microsoft Windows Server 2022	Oct-26	Oct-31	Public
RedHat Enterprise Linux 7.0	Jun-24	May-29	Legacy
RedHat Enterprise Linux 8.0	May-24	May-29	Legacy
RedHat Enterprise Linux 9.0	May-27	May-32	Public
RedHat Enterprise Linux 8.0 for SAP	May-25	Oct-27	Legacy
Linux Debian Standard 10	Jun-24	Jun-29	Legacy

Linux CentOS 7	Dic-21	Dic-21	No Available
Linux CentOS 8	Jun-24	Jun-24	Legacy (6 months)
Linux Ubuntu Server 16.04 LTS	Abr-21	Abr-28	Legacy
Linux Ubuntu Server 18.04 LTS	May-23	Abr-30	Legacy
Linux Ubuntu Server 20.04 LTS	May-25	Abr-32	Public
Rocky Linux 9	May-27	May-32	Public
Alma Linux 9	May-27	May-32	Public
SUSE Linux Enterprise Server 12	Oct-24	Oct-30	Legacy
SUSE Linux Enterprise Server 12 for SAP HANA	Oct-24	Oct-30	Legacy
SUSE Linux Enterprise Server 15	Jul-31	Jul-37	Public
SUSE Linux Enterprise Server 15 for SAP HANA	Jul-31	Jul-37	Public

a. Available Databases

Microsoft SQL Server 2019 Standard
Microsoft SQL Server 2017 Standard
Microsoft SQL Server 2012 Standard

2.37 Creation of Virtual Machines from an OVA/OVF Image

Claro Enterprise Solutions enables the CUSTOMER to create a virtual machine from an image .OVA / .OVF / .ISO format, subject to the following conditions:

a. Claro Enterprise Solutions will not provide technical support for licenses that are no longer supported by the manufacturer, such as WINDOWS SERVER 2008.

b. Any virtual machine created from an external image that includes the use of licensed Operating Systems will be billed by Claro Enterprise Solutions. The use of out-of-support licensing does not exempt the corresponding billing by Claro Enterprise Solutions.

2.38 Security/Vulnerability Management/Patch Management

Claro Enterprise Solutions provides security updates regularly. The Customer can access these updates through the software distribution server. The Customer will install these updates by self-service within three months of release and complete their activation by rebooting the system.

If the Customer fails to comply with the installation, Claro Enterprise Solutions reserves the right to actively install updates as part of an "emergency patch process" at the Customer's expense and inform the Customer of this measure.

3. TERMS AND CONDITIONS OF USE OF MICROSOFT SOFTWARE

This Section governs the use of Microsoft software, hardware, printed materials, and related online electronic documentation (individually and collectively the "Microsoft Products") which Customer may elect to utilize as part of the Service. The Customer's right to use Microsoft Products is subject to the contract terms concluded with Claro Enterprise Solutions and the compliance and acceptance of the following terms and conditions, which may not be modified, altered, or varied by Customer.

3.1 Definitions

"CUSTOMER Software" allows a Device to access or use the services or functionality offered by the Server Software.
"Device" refers to each computer, workstation, terminal, handheld PC, pager, telephone, or personal digital assistant.
"Licensing Site" means http://www.microsoft.com/licensing/contracts or a successor site.
"Online Services" means Microsoft-hosted services to which Customer subscribes under this Agreement. It does not include software and services provided under separate license terms. "Smartphone," server, or other electronic devices.
"Server Software" is software that provides services or functionality on a computer that acts as a server.
"Software Documentation" is any end-user documentation included with the server software.
"Redistribution Software" is the software described in point 4 ("Using Redistribution Software") below.
"Use Rights" means the license terms and terms of service for each Product published on the Licensing Site and updated from time to time. The Use Rights supersede the terms of any end user license agreement that accompanies a Product. License terms for all Products are published in the Product Terms. Terms of service for Online Services are published in the Online Services Terms.

3.2 License Grant; Ownership of Products

A subsidiary of Microsoft Corporation (collectively, "Microsoft") licenses the temporary use of the Products to the CUSTOMER (the "Products"). All ownership rights and intellectual and industrial property rights in and to the Products (and their components, including, without limitation, images, photographs, animations, video, audio, music, text, and applets incorporated into the Products) are

the property of Microsoft or its suppliers. Products are protected by intellectual property laws and international intellectual property treaties, as well as other intellectual and industrial property laws and treaties. Possession of, access to, or use of the Products does NOT convey to the CUSTOMER any ownership rights in the Products, nor any intellectual or industrial property rights therein. Use of CUSTOMER Software

The Customer may use the CUSTOMER Software installed on applicable Devices only following the instructions and only regarding the Services provided by Claro Enterprise Solutions. The terms of this Section 3 permanently and irrevocably supersede the terms of any other Microsoft End User License Agreement submitted in electronic form as part of Customer's use of the CUSTOMER Software.

3.3 Use of Distribution Software

Concerning the services provided by Claro Enterprise Solutions, the Customer may have access to particular "example," "redistributable" software or software development software ("SDK") code and tools (individually and collectively "Redistribution Software") by which the CUSTOMER MAY NOT USE, MODIFY, COPY OR DISTRIBUTE ANY SOFTWARE OF REDISTRIBUTION UNLESS CUSTOMER EXPRESSLY ACCEPTS AND COMPL WITH CERTAIN ADDITIONAL TERMS CONTAINED IN THE RIGHTS OF USE OF THE SERVICE PROVIDER ("SPUR") APPLICABLE TO THE CUSTOMER, WHICH WHERE APPLICABLE WILL BE HANDED OVER TO CUSTOMER. Microsoft does not allow the use of any Redistribution Software unless the Customer accepts and complies with such additional terms provided by Claro Enterprise Solutions.

The Customer is expressly prohibited from using the software in so-called high-risk environments. Examples of high-risk use include but are not limited to airplanes or other modes of human mass transportation, nuclear or chemical facilities, or life support systems.

3.4 Copy

The Customer may NOT make any copies of the Microsoft Products, unless (a) Customer makes a copy of the CUSTOMER Software on a device with the express permission of Claro Enterprise Solutions; and (b) Customer makes copies of specific Redistribution Software following point 4 (Use of the Redistribution Software). Customer must erase and destroy all CUSTOMER Software and/or Redistribution Software upon termination or termination of the Agreement between Customer and Claro Enterprise Solutions, when the latter notifies Customer to do so, or when Customer transmits a Device to another person or entity, whichever comes first. The customer may not copy any printed materials that accompany Microsoft Products.

3.5 Limitations of Reverse Engineering, Decompilation, and Disassembly

The Customer may NOT reverse engineering, decompile, or disassemble Microsoft Products, except and only to the extent that such activity is expressly permitted by applicable law, despite this limitation.

3.6 No rent

Customer may not rent, borrow, donate, or directly or indirectly transmit or distribute the Microsoft Products to any third party. Customer may not allow any third party to access and/or use the functionality of the Products for a purpose other than accessing the functionality of the Microsoft Products in the form of software services, following the terms of this contract and any contract between Customer and Claro Enterprise Solutions.

3.7 Termination

Claro Enterprise Solutions may terminate the CUSTOMER's rights to use Microsoft Products without prejudice to any other right if the Customer does not comply with these terms and conditions. In the event of termination or cancellation of the contract between Claro Enterprise Solutions and the Customer or the agreement between the Customer and Microsoft, under which the Microsoft Products are licensed, the Customer must stop using or accessing Microsoft Products and destroy all copies of the Microsoft Products and all components.

This service is a separate service from virtual servers, so if Customer cancels a virtual server, Customer will also have to cancel the associated Microsoft license independently; otherwise, Customer will continue to be billed.

Microsoft may suspend use of an Online Service without terminating this Agreement during any period of material breach. Microsoft will give the customer notice before suspending an Online Service when reasonable.

Microsoft may modify, discontinue, or terminate a Microsoft Product in any country or jurisdiction where there is any current or future government regulation, obligation, or other requirement, that (1) is not generally applicable to businesses operating there; (2) presents a hardship for Microsoft to continue offering the Product without modification; or (3) causes Microsoft to believe these terms or the Product may conflict with any such regulation, obligation, or requirement. If Microsoft terminates a subscription for regulatory reasons, Customer will receive, as its sole remedy, a credit for any subscription fees, including amounts paid in advance for unused consumption for any usage period after the termination date.

3.8 GUARANTEES AND RESPONSIBILITIES

THE MICROSOFT PRODUCTS ARE PROVIDED WITHOUT WARRANTY, LIABILITY, OR RESOURCES ON THE PART OF MICROSOFT. OF COURSE, MICROSOFT (OR ANY OF ITS AFFILIATES OR SUBSIDIARIES) DOES NOT PROVIDE THE CUSTOMER WITH ANY WARRANTY, NOR DOES IT ASSUME LIABILITY TO THE CUSTOMER FOR DAMAGES, DAMAGES, AND/OR ANY APPLICABLE LEGAL REMEDIES.

3.9 Product Technical Support

Claro Enterprise Solutions shall provide technical support to the CUSTOMER solely to ensure proper installation of the contracted Microsoft licenses. Assistance related to the use or operation of such software is expressly excluded from Claro Enterprise Solutions 's scope of support.

NO-FAULT TOLERANCE

THE MICROSOFT PRODUCTS MAY CONTAIN TECHNOLOGY THAT IS NOT FAULT-TOLERANT AND IS NOT DESIGNED, MANUFACTURED, OR INTENDED FOR USE IN ENVIRONMENTS OR APPLICATIONS WHERE PRODUCT FAILURE COULD RESULT IN DEATH, PERSONAL INJURY, OR SERIOUS PHYSICAL OR ENVIRONMENTAL DAMAGE.

3.10 Export Restrictions

The Microsoft Products are subject to U.S. export jurisdiction. The Customer must comply with applicable laws, including U.S. Export Administration Regulations, International Traffic in Arms Regulations, and user restrictions, end-use and destination restrictions issued by the United States and other governments. For additional information, see http://www.microsoft.com/exporting/.

3.11 Liability for non-compliance

In addition to any liability Customer may have to Claro Enterprise Solutions, Customer agrees that it will be legally liable directly to Microsoft for any breach of the terms and conditions set forth in this Section 3.

4. TERMS AND CONDITIONS OF USE OF RED HAT SOFTWARE

This Section governs the use of RedHat Enterprise Linux which Customer may elect to utilize as part of the Service. The Customer's right to use RedHat Enterprise Linux is subject to the contract terms concluded with Claro Enterprise Solutions and the compliance and acceptance of the following terms and conditions, which may not be modified, altered, or varied by Customer.

By licensing RedHat Enterprise Linux, the Customer accepts the terms and conditions of the Software.
Subscription Agreement, which is available at the following URL: www.redhat.com/licenses/cloud_cssa/. Red Hat further denies:

a. Any warranty concerning Red Hat Inc. software.
b. Liability for any damage, whether direct or indirect, incidental, special, punitive, or consequential, and any loss of profits, revenue, data, or data usage, resulting from Customer's use of Red Hat, Inc.

5. TERMS AND CONDITIONS OF USE OF SUSE SOFTWARE

This Section governs the use of SUSE Linux Enterprise, which Customer may elect to utilize as part of the Service. The Customer's right to use SUSE Linux Enterprise is subject to the contract terms

concluded with Claro Enterprise Solutions and the compliance and acceptance of the following terms and conditions, which may not be modified, altered, or varied by Customer.

By licensing SUSE Linux Enterprise, the CUSTOMER accepts the terms and conditions of the Software. Subscription Agreement, which is available at the following URL: https://www.suse.com/licensing/eula/ and https://www.suse.com/company/legal

SUSE also denies:

a. Any warranty concerning the software of SUSE, LLC.

b. Liability for any damages, whether direct or indirect, incidental, special, punitive, or consequential, and any loss of profits, income, data, or data usage, resulting from Customer's use of the SUSE, LLC software.

6. CUSTOMER RESPONSIBILITY

6.1 General Responsibilities of the CUSTOMER

a. The CUSTOMER shall appoint a central and qualified contact person for customer support and ensure the replacement of such contact when necessary. The CUSTOMER must ensure the availability of this contract 24 hours a day, 7 days a week. The CUSTOMER shall keep the designation of the point of contact up to date.

b. The CUSTOMER shall provide all software licenses and other protected content required for the provision of the services unless Claro Enterprise Solutions has expressly agreed in writing to provide the corresponding content.

c. The CUSTOMER declares that it agrees to exchange information via email and that it will always provide a current email address. The CUSTOMER is aware that essential information for the provision of services, such as access data, information on service modifications, and legal conditions, is sent exclusively by email.

d. The CUSTOMER shall be responsible for verifying whether the data transferred by the CUSTOMER in connection with the use of the service constitutes personal data and whether the processing of such personal data is permitted. To the extent that the CUSTOMER wishes personal data to be processed, the CUSTOMER must sign a data processing agreement based on Claro Enterprise Solutions' sample agreement, which will be provided by Claro Enterprise Solutions.

e. The CUSTOMER warrants that it will not store any content in the contractual storage space or make it available online if the provision, publication, or use of such content violates applicable laws or third-party rights; this applies to defamatory, hate-inciting, or extremist content.

f. The CUSTOMER shall be responsible for verifying and ensuring compliance with all legal provisions, laws, regulations, and industry-specific requirements that are relevant and applicable in connection with the use of the service. This includes compliance with confidentiality obligations, such as those arising from professional activities. The CUSTOMER must confirm that confidentiality-relevant data will only be stored when effective authorization exists.
g. The CUSTOMER shall inform its users about the regulations of this service as well as the "service specifications and additional terms and conditions," especially regarding the licensing terms for operating systems and cooperation duties and shall ensure their compliance.

6.2 CUSTOMER Responsibilities During Initial Provisioning

a. The CUSTOMER must register in the Cloud Store before contracting the service. Once the registration is completed, the CUSTOMER accepts the terms and conditions of the Cloud services, after which the service contract option will be enabled.
b. The CUSTOMER may choose the following contract options for each Virtual Data Center:
   • On-demand, with monthly billing based on service usage.
   • Resource pool of compute resources (vCPU, RAM, Disk) with a commitment term of 1, 12, 24, or 36 months, billed monthly. Additional charges apply for consumption of variable elements such as operating systems, network transfer, and others.
c. Upon completing the service contracting process, the CUSTOMER will receive a confirmation email with the details of the purchase.
d. The CUSTOMER will receive a welcome email containing the necessary information to access the service, including the Administrator username and the URL (https://sso.clarocloud.com) to set the access password for the Self-Service Portal. Passwords must not be shared with third parties.
e. If the CUSTOMER does not receive any of these emails, they may contact the support center to request that the emails be resent.
f. The CUSTOMER is responsible for the proper use and safeguarding of the administrative credentials (usernames and passwords), as well as for handling customer information within the service. Claro Enterprise Solutions is not responsible for unauthorized access to the Service.
g. The CUSTOMER must provide Claro Enterprise Solutions with all necessary information to configure the optionally requested private network connection. For IP-VPN / MPLS: The CUSTOMER shall provide an IP address segment and subnet mask from the CUSTOMER's network, which will be used to connect the T1 Edge Gateway with the customer's IT environment.

6.3 Customer Responsibilities During Use of the SERVICE

a. The CUSTOMER is responsible for managing their own capacity and must expand or reduce their resource capacity at the Virtual Data Center (Resource Pool) level through the Control

Panel or their sales representative, taking into consideration the number of resources and the minimum contracting periods.

b. The CUSTOMER must protect the Virtual Data Centers, operating systems, and applications within their virtual machines against third-party attacks and misuse and keep them free of malicious software (malware). The CUSTOMER shall immediately install all relevant security-related operating system patches through the self-service portal. In addition, the CUSTOMER must protect the virtual machines in the Virtual Data Center by configuring the virtual firewall of the T1-Edge Gateway and Load Balancers against misuse and external attacks and must always update the T1-Edge Gateway and Load Balancers to the currently published version (re-implementation).
c. The CUSTOMER will independently manage user and administrator permissions and roles within their Virtual Organization (vOrg). Through the Self-Service Portal, the CUSTOMER may create, delete, and modify users, as well as assign any of the predefined access roles.
d. The CUSTOMER will monitor the provisioning and usage of the contracted resources.
e. The CUSTOMER will not delete or modify any required system user, particularly those created by Claro Enterprise Solutions (for example: Managed Services users).
f. The CUSTOMER must not uninstall VMware Tools (VM-Tools), which support the guest operating system within their virtual machines. VMware Tools are required to ensure the service quality of the virtual machines.
g. The CUSTOMER must not delete the Firewall rule associated with the shared services network ("Shared Services") accessible from the Control Panel.
h. When necessary, the CUSTOMER shall be available to coordinate with Claro Enterprise Solutions for handling security changes and emergency cases.
i. The CUSTOMER shall use the operating system images provided by Claro Enterprise Solutions exclusively within the SERVICE. Downloading or transferring these images to other environments is prohibited.
j. The CUSTOMER shall administer the Operating System used in virtual machines and other components of the Service, including:

   • Installation and updating of antivirus and antimalware security suites.
   • Installation of security patches.
   • Configuration of firewall rules and ensuring their logical consistency.
   • Support and management of any other installed software.
   • Clock synchronization.
   • Hardening measures and management of technical vulnerabilities.
   • Protection against targeted cyberattacks.
   • Encryption of information and safeguarding of encryption keys.
   • Migration to another operating system before the manufacturer declares it deprecated or before Claro Enterprise Solutions decides to discontinue offering or supporting it as part of the SERVICES.

k. The CUSTOMER acknowledges and agrees that the information stored within the SERVICE resides in a shared storage system in Claro Enterprise Solutions' Data Centers.
l. The CUSTOMER must back up their data once per day in an appropriate manner so that it can be recovered at a reasonable cost.
m. When using the Backup Service (Backup as a Service), the CUSTOMER must periodically verify the status of backups through the Self-Service Portal and perform periodic recovery tests under their own responsibility.
n. The CUSTOMER shall responsibly manage Snapshots in their virtual machines. Snapshot functionality is not a backup mechanism. Claro Enterprise Solutions only allows one concurrent Snapshot per virtual machine.
o. If necessary, the CUSTOMER shall implement disaster recovery concepts at the virtual machine and application level under their own authority.
p. When using vCloud Availability, the CUSTOMER must periodically verify the status of replicas through the Self-Service Portal and perform periodic failover tests under their own responsibility.
q. The CUSTOMER is responsible for the use of the service, including all activities, regardless of whether they are performed by the CUSTOMER, employees, or third parties (e.g., end users). Claro Enterprise Solutions is not responsible for unauthorized access to the service.
r. The CUSTOMER accepts that Claro Enterprise Solutions reserves the right to suspend the CUSTOMER's username and password for access to the Self-Service Portal at any time if it determines that any CUSTOMER user is violating or may potentially violate the service's security conditions.
s. The CUSTOMER accepts that Claro Enterprise Solutions reserves the right to request or require the CUSTOMER to change the password used in the service.
t. The CUSTOMER must immediately inform Claro Enterprise Solutions of any change in the authorized user information (service administrator) that may compromise security.
u. The CUSTOMER may change their service access password, as well as the passwords of CUSTOMER-authorized users, whenever required.
v. The CUSTOMER may request support for access and basic use of the Self-Service Portal from the support center.
w. The CUSTOMER is responsible for the information, operation, backup, maintenance, and use of their information within the service.
x. The CUSTOMER is responsible for classifying and labelling the information and information assets associated with and contained in their service.
y. The CUSTOMER must configure their SERVICE to enable communication to the Internet or may request assistance from the SUPPORT CENTER.
z. When using the service, the CUSTOMER shall not infringe the rights of others and shall not store information that violates any third-party intellectual property rights.
aa. When using the service, the CUSTOMER shall not damage, interfere with, clandestinely intercept, or expropriate any system or software.

bb. The CUSTOMER is responsible for complying with applicable local and/or foreign laws regarding content deletion.

cc. The CUSTOMER is responsible for paying any charges and/or expenses incurred for resource consumption through the Self-Service Portal or APIs, including but not limited to:
• Network, Compute, and Storage resources.
• API calls to the Service, consumption reports, and any solution available through the SERVICE.
• Actions or configurations performed by the SERVICE ADMINISTRATOR or any CUSTOMER-created users.
• Any impact to the CUSTOMER's services or functionality resulting from actions performed by the CUSTOMER, the SERVICE ADMINISTRATOR, or SERVICE users, provided such actions are executed through the Self-Service Portal or API calls to the SERVICE.

dd. The CUSTOMER shall perform actions and configurations of the functionalities available within the SERVICE's Self-Service Portal.

ee. The CUSTOMER shall indemnify, defend, and hold Claro Enterprise Solutions harmless from any claim, demand, and/or legal action arising from the use of the SERVICE by the CUSTOMER or any third parties related to the CUSTOMER, whether such use causes damage, alteration, and/or modification to the network, media, and/or infrastructure through which Claro Enterprise Solutions provides the SERVICE, or involves the use of the SERVICE for illicit activities, including but not limited to pornography, cryptocurrency mining, cybercrime, misuse of personal data, execution or propagation of malware such as ransomware or any of its variants.

ff. The CUSTOMER shall provision and monitor the use of the compute resources contracted within their subscriptions.

gg. The CUSTOMER is responsible for registering and monitoring events related to the contracted SERVICE.

hh. Due to the self-service nature of the Service, provisioning, configuration, association, access, and deletion of information are the CUSTOMER's responsibility.

ii. The CUSTOMER may use their own licensing if they comply with the applicable vendor licensing requirements, acknowledging that Claro Enterprise Solutions will not provide technical support for such licensing.

jj. The deletion or removal of virtual machines configured by the CUSTOMER is irreversible. Once deleted, the associated information and configuration cannot be recovered.

6.4 Customer Responsibilities for Service Termination

a. The CUSTOMER must perform an independent backup of all application data stored in the SERVICE by downloading it before the contract ends. Claro Enterprise Solutions will disable the CUSTOMER's access and delete the CUSTOMER's application data from the Data Center as of

the day the contract ends or the day the CUSTOMER cancels the SERVICES through the Self-Service Portal.

b. It is the CUSTOMER's responsibility to back up the information stored in the SERVICE before performing any deactivation or cancellation. Service deletion may take up to 48 hours. Once the SERVICE has been terminated, the process is irreversible, and Claro Enterprise Solutions is not responsible for any loss or deletion of CUSTOMER-owned information.

6.5 Claro Enterprise Solutions Responsibilities

Claro Enterprise Solutions is responsible for fulfilling the following obligations in the provision of the SERVICES:

a. Claro Enterprise Solutions will guide and support the CUSTOMER during the configuration of the credentials and access permissions required by the CUSTOMER to establish a connection with the SERVICE.
b. Claro Enterprise Solutions will address incident reports submitted by the CUSTOMER through the Support Center.
c. Claro Enterprise Solutions will protect data records by complying with the controls established in its Integrated Management System for information security, including the handling of controlled access and information logs within its technological platforms.
d. Claro Enterprise Solutions shall operate, administer, and control the components of the operating system of physical servers (ESXi), the virtualization layer, the network layer, and the physical security of the facilities where the SERVICE operates.
e. Claro Enterprise Solutions will notify the CUSTOMER of major preventive and corrective maintenance windows that may affect the availability of the SERVICE. This infrastructure is composed of the hardware, software, networks, and facilities where the SERVICE is executed. Claro Enterprise Solutions ensures the application of updates, security patches, backups of service management systems, security policies, event monitoring, hardening measures, and technical vulnerability management for the security of this Infrastructure and maintains responsible control over network segregation.
f. Claro Enterprise Solutions guarantees the availability, integrity, and confidentiality of the digital data processed, presented, retained, and stored when using the SERVICE, provided that the CUSTOMER complies with the responsibilities for the use of the SERVICE and remains current and without outstanding payments for the corresponding fees.
g. Claro Enterprise Solutions guarantees the security of the infrastructure that comprises the hardware, software, networks, and facilities where the SERVICES are executed, through:
   • Applying updates to the various components of the SERVICE.
   • Implementing patches for security vulnerabilities.
   • Performing backups of SERVICE management systems.

- Applying, reinforcing, and maintaining updated security policies.
- Event monitoring, supported by proper clock synchronization.
- Hardening and reinforcement measures.
- Technical vulnerability management.
- Control over network segregation.

h. Claro Enterprise Solutions will notify the affected CUSTOMER of any identified security incident that impacts the availability, integrity, or confidentiality of the service and their personal data. Claro Enterprise Solutions will provide a report defined by Claro Enterprise Solutions upon request. The report will include a summary of the event and the solution implemented.

i. Claro Enterprise Solutions and its SERVICE-related providers operate under best practices and standards for information security and privacy, which are validated through independent reviews of the Data Center's current certifications, in accordance with international Privacy Principles and the Principles, Duties, and Obligations established by Law.

j. Claro Enterprise Solutions will report on the activities it considers to constitute a violation of the law. In cooperation with the competent authorities, Claro Enterprise Solutions may disclose CUSTOMER information to support any investigation or complaint.

k. If Claro Enterprise Solutions detects security violations that it considers posing a risk to its infrastructure, Claro Enterprise Solutions may temporarily or permanently suspend, partially or completely, the SERVICE contracted by the CUSTOMER, depending on the severity of the event, without any liability for Claro Enterprise Solutions.

The CUSTOMER acknowledges and agrees that Claro Enterprise Solutions is not responsible for:

• Improper configuration of the SERVICE by the CUSTOMER or the SERVICE ADMINISTRATOR.

• Configuring credentials and access permissions for the CUSTOMER's Self-Service Portal accounts within the SERVICE.

• Providing support for native Kubernetes clusters or CentOS, Ubuntu, and Debian operating systems, as these are open-source licensed.

• Verifying or evaluating damaged files or files containing malicious code, or repairing, disinfecting, or decrypting any file sent by the CUSTOMER.

• Information, data transmission, data loss, access times, or any access restrictions to a network and/or a specific server connected to the Internet.

• SERVICE failures caused by incompatibility between the SERVICE and any other service contracted by the CUSTOMER.

• The CUSTOMER's configuration and use of the SERVICE, including any loss, corruption, or damage to information.

• Damage or issues with the CUSTOMER's computing equipment or installed software, or problems related to the CUSTOMER's contracted Internet access. Claro Enterprise Solutions is not responsible for software installation or data migration between virtual machines contracted by CUSTOMER. The CUSTOMER acknowledges that the data is their property and responsibility, and therefore they are solely responsible for its migration, protection, and backup.

7. PRICING

7.1 Services without Minimum Subscription Period

Usage-based billing is based on the allocation of computing resources (CPU, RAM, and Disk). Usage is calculated from the moment of creation of each virtual machine added to the Service. There is no minimum required usage. Usage is calculated in five (5) minute increments, as follows:

a. For On-Demand Services, the RAM and vCPU resources: Each minute of the month during which the virtual machine is in the "on" state.

b. For On-Demand Services Microsoft and Red Hat Storage and Operating Systems: Each hour of the month during which the virtual machine is contracted and enabled in the powered-on state.

c. SUSE Linux Enterprise Operating Systems: Charged monthly regardless of the virtual machine's state.

d. The CUSTOMER may activate or deactivate the virtual machines to start or stop their use and billing.

7.2 Services with Minimum Subscription Period

Customers must renew services with a minimum subscription period with a minimum notice of 30 days before the end of the then-current term. The following conditions apply:

a. The minimum subscription periods for the Resource Pool Service are 1 month, 12 months, 24 months, and 36 months. Customers may choose the billing for the minimum periods of contracting the Service either with a monthly payment or a one-time fee in advance.

b. For Resource Pool Services, a total of 720 hours per month is considered for calculations of monthly vCPU, RAM, and Disk charges.

c. For Resource Pool Services with a minimum contracting period, reductions in the number of vCPU, RAM, and Disk are not possible.

d. The minimum contracting capacity for each Resource Pool is 20 vCPUs, 50 GiB RAM, and 200 GiB Disk.

e. For Resource Pool Services with a minimum subscription period, increases in the number of vCPU, RAM, and Disk are possible. The minimum subscription period starts again with each addition.

f. In the case of Resource Pool Services with a minimum contract term, early termination is permitted. The CUSTOMER is required to pay Claro Enterprise Solutions, with a single lump-sum payment, the amount corresponding to the monthly SERVICE fee multiplied by the number of months remaining in the minimum contract term. The CUSTOMER acknowledges that they are

solely responsible for the backup and migration of their information and agrees that, to access, back up, or retrieve their information, they must first pay the applicable early-termination charges.

g. The CUSTOMER is responsible for renewing the SERVICES with a minimum contract term before the end of the current contract period.

7.3 Pricing Methods and Calculation of Payments

a. For Service items with usage-based pricing (such as usage of vCPU, RAM, Disk, VPN, licenses, and others), actual use is measured in billing units defined at 5-minute intervals. Customer is billed as an average usage amount per calendar month for each price item related to each Org-VDCs contracted by the CUSTOMER.

b. The Resource Pool Service has an equivalence of 2 GHz for each vCPU.

c. For Service items with usage-based pricing, the Coordinated Universal Time (UTC) standard is used as a single time reference (in all Enterprise Claro Cloud regions) for recording the start and end date and time of the Services to calculate monthly usage.

d. Public IP addresses will be billed only when shown as used in the Self-Service Portal. Public IPs used are billed uniquely regardless of whether they are configured for different uses (e.g., Primary, NAT, SNAT, etc.).

e. In the case of data transfer, the outgoing traffic per calendar month of each Org-VDC will be measured and billed to the customer. There is no cost for incoming traffic.

f. In the case of the Backup Service, the actual maximum amount of data stored will be measured daily and billed as an average usage amount per calendar month.

g. The use of Microsoft and Red Hat operating systems will be measured by OS instance (from the initial provisioning of a virtual machine to the time of deletion of a virtual machine). It will be billed as the monthly sum of all operating systems managed in an org-VDC. The use of SUSE operating systems will be billed the full monthly charge for an individual virtual machine, even if it is deleted during the month.

h. Managed Services will be billed for each ORG-VDC contracted under the modality of managed services. A charge applies to adding the monthly fixed base fee and the variable quota calculated according to the Customer's monthly usage of VCPU, RAM, and DISK. Billing will occur as soon as the CUSTOMER contracts the Service in the Control Panel.

i. The use of protection with vCloud Availability will be measured and charged by protected virtual machines. If a vApp is covered, all saved virtual machines in that vApp are subject to charges.

- For a VM that is protected and unprotected without moving it from the destination (Example: migration, failover, switching to another vApp or Region) and protected again, one protection is charged per month.
- Two protections are charged for a protected virtual machine, failover to a target region and then protected again.
- Two protections are charged for a protected virtual machine moved to another vApp or Target Region and then protected again.

Storage consumption in the target Org-VDC for the first replication and virtual machine recovery point instances is charged at the storage price of the target Region. Because storage for recovery point instances is not limited to the size of storage ordered within the Resource Pool type OrgVDCs, storage consumption that exceeds the storage (disk) size of the Resource Pool will be charged based on the price items per storage usage.

j. For migrations with vCloud Availability, storage consumption in the Org-VDC in the target Region is charged based on the storage usage price items in the Target Region, if the migration is active and the virtual machine has not been failover or failover. During migration, there is no cost to use vCloud Availability. Claro Enterprise Solutions subsequently reserves the right to charge for vCloud Availability protections for each protected VM.

k. Billing will occur monthly on a postpaid model (billing month = month of service delivery +1) for one-time, monthly, and usage-based charges. Claro Enterprise Solutions has the right to revise billing for one-time charges and/or monthly charges to advance billing (billing month = month of service delivery). Claro Enterprise Solutions will inform the Customer in advance of a planned change in billing.

l. All pricing information does not include applicable local taxes.

7.4 Price List

All public prices are expressed in local currency without taxes. The price list is public and can be consulted at https://www.usclarocloud.com/portal/us/cld/products/infrastructure/enterpriseclarocloud/quote/ Claro Enterprise Solutions reserves the right to modify the price list and specifications of the services at any time, without notice, and is not responsible for typographical or other errors nature that this list might have.

8. SERVICE LEVEL

8.1 Service Demarcation

Claro Enterprise Solutions' responsibility for the specified Services ends at the service demarcation and transfer point. The service demarcation point is the point of entry from the data center to the Internet, or the point of entry to the CUSTOMER's external and/or internal private network connection within the Data Center.

8.2 Maintenance Work

Claro Enterprise Solutions performs maintenance work on a regular basis. The platform is redundant, so regular maintenance activities do not cause interruptions. If maintenance work results in an interruption, Claro Enterprise Solutions will notify the CUSTOMER in advance, except for maintenance classified as urgent. Claro Enterprise Solutions aims to minimize any interruptions. Maintenance work is not considered downtime and therefore is not counted in the monthly availability calculation.

8.3 Availability Calculation

Operating hours: The operating hours refer to the period during which the Services are available.

Support hours: The support hours refer to the period during which technical support is provided, and incidents affecting system availability are processed.

Maintenance window: The CUSTOMER acknowledges that the hardware and software infrastructure that makes up the platform used by Claro Enterprise Solutions to operate the Services must be kept efficient and up to date. The platform is configured in a redundant manner so that maintenance work can be performed during ongoing operations without service interruption. Claro Enterprise Solutions will notify the CUSTOMER if maintenance work is required. Maintenance work will not be considered downtime for availability calculation.

Availability Formula Availability is expressed as a percentage, known as the availability percentage, and is calculated as follows:

$$\frac{(Total\ Service\ Minutes) - (Total\ Downtime\ Minutes)}{Total\ Monthly\ Servicio\ Minutes}$$

Definitions
Total Service Minutes: The number of minutes per month = 60 minutes × 720 hours.

Total Downtime Minutes: The number of minutes in the previous month during which a Service component was unavailable, minus the number of minutes corresponding to excluded events during the same period. If the service purchase (contractual relationship) is less than 30 days old, only the downtime minutes occurring from the start of the contractual relationship will be calculated. Downtime begins when the CUSTOMER registers and opens a failure case with Claro Enterprise Solutions support. After investigating and repairing the failure, Claro Enterprise Solutions will contact the customer to notify them that the Service may be used again. This will be considered at the end of the downtime period, unless the customer does not confirm the repair and there is sufficient evidence that the issue persists.

Excluded Events: The occurrence of any of the following is sufficient for exclusion:

a. Downtime caused by maintenance work and changes.
b. If the CUSTOMER's service poses a risk or degradation to third-party services or to Claro Enterprise Solutions' platform (e.g., due to a DDoS attack), Claro Enterprise Solutions reserves the right to deactivate the affected service without prior notice until the risk or degradation is resolved. Downtime caused by this action will not be considered in the availability calculation.

c. Incidents, downtime, and issues attributable to the CUSTOMER, its employees, or representatives.
d. Complete failure of a Data Center in a region. In such an event, service levels will be suspended for services in that region (Data Center) and for the Self-Service Portal until they become available again. Claro Enterprise Solutions will apply all resources and efforts within its reach to minimize potential loss of the Self-Service Portal and Data Centers.
e. Issues beyond Claro Enterprise Solutions' reasonable control.
f. Failures or omissions in equipment, cabling, software, or other services not provided by Claro Enterprise Solutions.
g. Service suspension due to CUSTOMER's outstanding payments.
h. Time elapsed when Claro Enterprise Solutions requires information from the CUSTOMER or confirmation that the service has been restored, and no response is received.
i. Any failure caused by the CUSTOMER's Service Administrator.
j. Any failure caused by a virus or external agent negligently introduced by the CUSTOMER or any of its representatives.

8.4 Availability and Service Level

The Service modality contracted by the CUSTOMER will have a target service level according to the following table.

Component	Availability Percentage	Helpdesk Hours	Support Operations Hours
Self-service Portals and API's	99.95%	24hx7 days (Mon to Sun)	24hx7 days (Mon to Sun)
Platform	99.95%	24hx7 days (Mon to Sun)	24hx7 days (Mon to Sun)

8.5 Service Credits

If Claro Enterprise Solutions fails to meet the Availability Percentage in any of the monthly billing periods, the CUSTOMER shall be entitled to request the application of a service credit against the monthly billing for the affected services, in accordance with the following table:

.

Availability Percentage	Service Credit Rate
Below 99.99% but equal to or above 99.0%	10 %
Below 99.0% but equal to or above 95.0%	15 %
Below 95.0%	20 %

a. Service Credits are calculated as a percentage of the total charges for the affected Services paid by the CUSTOMER during the monthly billing cycle in which the Service unavailability occurred.
b. The CUSTOMER must request the Service Credits by providing all fault report numbers generated for the CUSTOMER by Claro Enterprise Solutions during the billing period in which the CUSTOMER demonstrates that the referenced fault caused the Service unavailability. Requests for Service Credits must be submitted no later than 30 days after the billing period in which the unavailability occurred.
c. Claro Enterprise Solutions reserves the right to verify the claims against the fault references cited by the CUSTOMER to obtain Service Credits, to ensure they are consistent with the applicable Service Level.
d. Service Credit application will be made in the billing cycle following the Service unavailability. If the unavailability occurs in the final month of the minimum service term, Claro Enterprise Solutions will issue a refund of the Service Credit to the bank account owned by the CUSTOMER.

The CUSTOMER must notify Claro Enterprise Solutions in writing of any dispute concerning any Service Credit, whether it has applied or not , no later than 30 days after the issuance of the corresponding invoice.

8.6 Technical Support for Incidents

Technical Support is activated at the time the Service subscription is created because of the contracting process. Claro Enterprise Solutions' support team will be available to manage all incidents in the local official language, from Monday to Sunday, 24 hours a day. The support team may be contacted exclusively by the CUSTOMER's authorized personnel (registered with Claro Enterprise Solutions) to open incidents by calling: +1 833 552 5276 or by email at: gnoc@usclaro.com. Claro Enterprise Solutions will open a ticket, assign a priority level, and classify the incident reported by the CUSTOMER as Critical or Non-Critical. Events classified as Critical are incidents that have an impact on the agreed service level of the platform. Events classified as Non-Critical are incidents that do not have an impact on the agreed service level of the platform.

Incident response times related to Service unavailability will be managed according to the Basic Support priority table:

Priority	Classification	Description	Time to Response
P1	Critical	Critical business impact and risk. All contracted services are unavailable.	30 minutes
P2	Critical	Significant business impact. Some contracted Services are unavailable.	2 hours

P3	Non-Critical	A component of the contracted Services is degraded or impacted.	8 hours
P4	Non-Critical	Change requests or general inquiries regarding the operation of the Services.	24 hours

At no additional cost, the CUSTOMER will have access to a basic monitoring dashboard for their Service and to the Service documentation, which includes the user manual published in the Help section of the Self-Service Portal: https://sso.clarocloud.com.