



CloudWave: Service Level Agreement

Last updated: December 3rd, 2020

This Service Level Agreement (SLA) is incorporated by reference into Customer’s Proposal and is subject to the Master Terms and Conditions. This SLA provides CloudWave’s commitment to Customer for the Services and Support selected by Customer from the options listed below, as set forth in Customer’s Proposal. During the Term and pursuant to the Proposal, CloudWave agrees to meet the Monthly Uptime Percentage (Service Level Target) for the Services type and Support levels selected by Customer. If CloudWave fails to meet the SLA target and subject to Customer’s compliance with the Agreement, if CloudWave does not meet the Monthly Uptime Percentage, then Customer is eligible for the Service Credit corresponding to its SLA, (Service Credits are listed below). Service Credits for partner or reseller services will only be provided by CloudWave if specifically included as part of a Proposal. In the event of a conflict between the terms of this SLA and the terms of the Master Terms and Conditions, the terms of this SLA will be governed solely as applied to Monthly Uptime Percentage and Service Credits.

Services Offerings included in the SLA:

- OpSus Live Puerto Rico

Service Level Agreement Options:

Customer’s Proposal has set forth Customer’s selection of one option from one or more of the groups of offerings below (Availability, Recoverability and Support). The combination of SLAs for the Customer selected offerings is referred to as the “package”.

Availability SLA Options:

Tier	Monthly Uptime %	WAN Connectivity		OpSus Live (Private Cloud)
		Minimum Diversity Requirement	Supported Types	
Single	>99.0%	Single Connection	Dedicated or VPN	Single Region

Recoverability SLA Options (All Services):

Tier	Compute			Storage	Operational Protection			Disaster Protection (Facility)			
	Instance	Backup	Retention	Retention	Protection	Source	Recovery	Protecti on	Mode	Source	Recovery
1. Silver	Single instance, DR from backups	Weekly	4 Weekly 12 Monthly	30 Daily 12 Monthly 7 Years (up to)	Single Volume	Backup	12 RTO 24 RPO	Single DC	Cold Site	Backup	12 RTO 24 RPO
2. Silver Plus	Single instance, DR from backups	Weekly	4 Weekly 12 Monthly	12 Hours 30 Daily 12 Monthly 7 Years (up to)	Single Volume	Snapshot	2 RTO 2 RPO	Single DC	Cold Site	Backup	12 RTO 24 RPO

Support and Managed Service SLA (All Services):

Feature		Support
Support Hours	8 AM – 5 PM	
	24 x 7 x 365	Standard

Feature		Support
Customer Advocate	CSM	Optional

Feature		Managed Services
Firewall	FW Internet to DC	Standard
	Manage Rules (<i>Host Based</i>)	Standard
	Instance Device/Appliance	Standard
	Device Management	Standard
Backup / Archive	Software	Standard
	Backup Management (<i>w. backup Target and retention</i>)	Standard
Utilities	Storage I/O Optimization	Standard (<i>MEDITECH Workloads</i>) Optional (<i>Other Workloads</i>)
Monitoring	Basic Availability	Standard
	Instance- Performance	Standard
	Instance- Capacity	Standard
	OS Performance	Standard
	Service Level Monitoring	Standard
	Alerting (<i>auto-ticketing</i>)	Standard
End Point Detection and Response	Software	Standard
	Manage (<i>Install, Configure, Support, Update</i>)	Standard
Software Patching	System Tooling (<i>Adobe, Flash, Chrome, etc.</i>)	Standard
	OS Patching	Standard
	Patch Management Software (<i>Install, Configure, Support, Update</i>)	Standard
	Zero Day Patching (<i>Customer assets</i>)	Standard
	Patching cycle (<i>Monthly or Quarterly</i>)	Standard
	HA patching (<i>Install, Configure, Support, Update</i>)	Optional
	OS Upgrades	Standard
	Security	IDS Software (<i>Host Based</i>)
IDS Management (<i>Install, Configure, Support, Update</i>)	Standard	
DDoS (<i>Network Based</i>)	Standard	
SIEM Software	Standard	
SIEM Management (<i>Install, Configure, Support, Update</i>)	Standard	
External Vulnerability Scanning	Standard	
External Vulnerability Scan Management (<i>Remediation</i>)	Standard	
Internal Vulnerability Scanning	Standard	
Internal Vulnerability Scan Management (<i>Remediation</i>)	Standard	
Hardened OS Image (<i>Baseline Configuration Management</i>)	Standard	
Compliance	Healthcare Compliant Provisioning * Only available in Public Cloud	Optional *
Load Balancer	Software	Standard
	Manage (<i>Install, Configure, Support, Update</i>)	Standard
SSL / Application Proxy	Software * Can be bundled with Load Balancer	Optional *
	Manage (<i>Install, Configure, Support, Update</i>)	Optional
Access	Management Environment MFA	Standard
	MFA End User Access * CW or Customer can provide, but feature is required for end user access	Optional * (<i>feature is required</i>)

Incident Response:

Applicable to all Support SLA options, but subject to the CloudWave Support Hours included with each tier.

Incident Priority	Response Times
-------------------	----------------

	<i>Initial Contact</i>	<i>Target Resolution</i>	<i>Communication Update</i>
Critical	<15 Mins	<6 Hours	Every 2 Hours
High	<1 Hour	<12 Hours	Every 4 Hours
Med	<8 Hours	<1 Business Day	Every 8 Hours
Low	<24 Hours	<3 Business Days	Every Business Day

Incident Description:

Priority	Description
Critical	Incidents affecting a large portion of the customer healthcare environment, causing production system failure (typically catastrophic), service interruption, outage, or system slowness resulting in significant loss of functionality (e.g., VDI access unavailability for entire hospital).
High	Incidents affecting more than 10 users causing production system failure, service interruption, degradation, or an outage affecting a subset of the customer’s healthcare environment.
Medium	Incidents affecting less than 10 users with no significant impact to the customer’s healthcare environment.
Low	Incidents affecting single users with no business interruption.

Monthly Uptime Percentage.

The actual Uptime Percentage is calculated as the total minutes of actual Services Availability divided by the total minutes in the affected month less Exclusions listed below.

Service Credits:

If the included Services do not meet the Monthly Uptime Percentage, Customer will be eligible to receive a Service Credit in the amounts set forth in the following tables by following the instructions below.

Single

Actual Uptime Percentage	Service Credit Percentage
<99.0 and >=98.0	10%
<98.0 and >=95.0	15%
<95.0	20%

Service Credit.

All approved Service Credits will be applied to the Customer’s next invoice. If a dispute arises regarding a Service Credit, CloudWave will use all available information (server logs, monitoring activity, configuration design, etc.) to make a good faith determination.

Calculation of Service Credit.

The Service Credit shall be calculated by multiplying the Service Credit Percentage due times the portion of the Monthly Recurring Charges applicable to the Services that failed to meet the Uptime Percentage. If Customer was unable to access all of the Services, the Service Credit Percentage will be calculated against the entire Monthly Recurring Charge for the applicable month.

Contract Termination.

If CloudWave fails to meet the Monthly Uptime Percentage of at least 95.0% in any three (3) consecutive months, then, in addition to the Service Credits due to Customer, the Customer may deem such failure to be a material breach by CloudWave under the Agreement and may pursue termination of the Agreement upon 15 days written notice. Customer’s sole and exclusive remedy, and CloudWave’s sole and exclusive liability, for CloudWave’s failure to meet the Monthly Uptime Percentage is the Service Credits and termination rights under this SLA.

Exclusions:

Exclusions from the Uptime Percentage calculation include downtime resulting from events that are not within the scope of CloudWave's obligations under this Agreement or that are not within the reasonable control of CloudWave, as well as the following:

- A Force Majeure Event as defined in the Master Terms and Conditions,
- Acts or omissions of the Customer or its employees, agents, contractors or representatives,
- The Customer's failure to follow implementation instructions or procedures issued by CloudWave,
- Use or failure of any Customer owned or provided hardware, software or other components used in connection with the Services,
- Failure of the Customer's internet provider, telecommunications circuit, or internet backbone outages, routing, or peering issues that prevents Customer access to CloudWave data center(s),
- Planned downtime for patching, maintenance, and/or infrastructure or application upgrades, conversions, and/or migrations,
- Emergency maintenance resulting from critical and time sensitive security exploits and threats, or other maintenance with the intent to protect the confidentiality, integrity, and availability of Customer's and/or CloudWave's systems and data, and/or safety or care of either parties' employees and/or associates,
- Downtimes resulting from critical security threats and exploits originating from the Customer site.