XMedius

SERVICE LEVEL AGREEMENT (SLA) – Voice Solutions

This document outlines XMedius' Service Level Standards and Security Standards with respect to the availability of the XMedius Voice Solutions (XM Connect, XM Hospitality and XM TeamQ) hosted by XMedius (hereinafter "XMedius Services") applicable during the term of the agreement related to such XMedius Services.

1. SERVICE LEVEL STANDARDS

1.1. Service Levels

XMedius will use commercially reasonable efforts to make the XMEDIUS Services available 99.9% or more of the time during any calendar month. Subject to the exclusions set forth below, an outage will be defined as any time where the XMedius Services are not available for normal use by customers due to a cause within the control of XMedius. The availability standard does not apply to any feature of the XMedius Service that XMedius identifies as a "beta" feature or service.

1.2. Service Credits

If XMedius fails to achieve the availability percentage above, Reseller will be eligible to receive a credit ("**Service Credit**") calculated as a percentage of Reseller's monthly fees in the calendar month when the applicable outage occurred. The Service Credits increase based on the amount of aggregate outage as follows:

Service Availability	Service Credit
Less than 99.9%	5%
Less than 98%	10%
Less than 97%	20%

Service Credits are non-transferable and will be issued in U.S. dollars. To receive a Service Credit, Reseller must contact XMedius in writing within thirty (30) days following the outage and demonstrate to XMedius' reasonable satisfaction that End User's use of the XMedius Service was adversely affected as a result of the outage. Any validated Service Credits will be applied against the next open invoice due to XMedius by Reseller. Any loss of service availability less than five (5) minutes in duration will not be included in the calculation of service availability.

1.3. Exclusions

The Service Level Standards only apply to unplanned outages. XMedius does not include in its calculation of downtime any time the system is offline (and XMedius Services are not provided) due to:

- Planned maintenance windows where notice of planned unavailability has been given at least two business days prior to the outage, unless in the case of emergency changes;
- Emergency maintenance not caused, directly or indirectly, by the negligence, gross negligence or willful misconduct of XMedius (or a party acting on XMedius' behalf);
- Force Majeure Events, including but not limited to, natural disasters, fires, flooding, labor disputes, riots, interventions by civil or military authorities, acts of war, declared or not, terrorism, failures of utilities and public services, and other unpredictable events;

- Actions or inactions on Reseller's part (including Reseller's failure to maintain the Required Components);
- Events arising from Reseller's or End User's systems;
- Denial of service or similar attacks, mail bombs, DNS resolution, domain name expiration, hardware failure, SYN attacks, ISP or Internet outages outside of XMedius' control; or
- Outages associated with any suspension, termination or expiration of the applicable agreement.

1.4. Sole Remedy

Notwithstanding any terms to the contrary in the applicable agreement, the Service Credits are Reseller's sole and exclusive remedy for any outage of (or service availability issues with respect to) the XMedius Services.

2. SECURITY STANDARDS

Specific to the XMedius provided Hosting Infrastructure, XMedius will only partner with hosting facilities that meet the following standards:

2.1. Platform Security

Use of redundant systems to eliminate single points of failure throughout the hosting infrastructure – enterprise class firewall systems, host and network intrusion protection systems, multiple Tier-1 internet service providers, high availability virtualization, and storage area networks.

2.2. Physical Security

Data centers that are actively monitored and guarded 24/7/365.

2.3. Employee Security

Employee access to passwords, encryption keys and electronic credentials is strictly controlled. Access to servers is restricted to authorized engineers and monitored regularly. Full time security staff are certified in all disciplines of information security.

2.4. SOC 2 / SSAE 16 Type II Certification

All Hosting Infrastructure providers must have an SOC 2 audit report from an independent auditor and use data centers that have passed an SSAE 16 Type II audit.

Notwithstanding anything to the contrary, XMedius reserves the right to update and change this SLA from time to time and will post a copy of the amended SLA on its website at the following address: https://xmedius.com/en/voice_sla/.

XMedius encourages Reseller to review the SLA periodically. If XMedius makes any substantial changes to the SLA, XMedius will notify Reseller by posting a prominent notice on its website or via email. Reseller will be deemed to have accepted the SLA, as amended, if it continues to use the XMedius Services after any such change.