Service Level Agreement

For SPARGO, Inc.

Parties Involved:

- **Internal IT Team**
- **Amazon Web Services (AWS)**
- **Microsoft Azure**

Effective Date: 06/16/2025
Review Period: Every 6 months
Scope: This SLA covers availability, reliability, and support for the meeting management system components, including integration of APIs, reporting systems, Ecommerce systems, and notification services.

---

1. Services Covered

- Integration APIs
- Reporting systems
- Ecommerce systems
- Authentication and Access Control
- Backend services hosted on AWS and Azure

---

2. Service Availability

Component	Platform	Availability Target
Integration APIs	Internal/Azure	99.9%
Reporting systems	Internal	99.5%

Component	Platform	Availability Target
Notification Services (Email)	AWS/Azure	99.99%
Authentication (SSO, OAuth)	Internal/AWS/Azure	99.5%

Note: AWS and Azure availability backed by their own SLA policies.

---

3. Response & Resolution Times

Severity	Description	Response Time	Resolution Time
Critical	System-wide outage	15 mins	4 hours
High	Partial outages, e.g., notification failure	30 mins	8 hours
Medium	Latency issues or minor API errors	1 hour	1 business day
Low	Non-critical issues or feature requests	1 business day	3–5 business days

---

4. Monitoring & Reporting

- **Internal Systems**: Monitored with Site 24x7 and LIBRE
- **AWS Services**: Monitored via **CloudWatch**
- **Azure Services**: Monitored via **Azure Monitor**
- **Monthly SLA Report**: Includes uptime, downtime, response times, and incidents logged.

---

5. Roles & Responsibilities

Internal IT:

- Manage Integration APIs
- Maintain security (SSO, access controls)
- Monitor integration points with AWS/Azure

AWS:

- Ensure reliability of SES/SNS or any Lambda/API Gateway-based microservices
- Issue incident notifications and SLAs per service documentation

Azure:

- Maintain up time of Azure-based services like Microsoft Graph API, Azure Functions, or Azure AD
- Handle Teams API integration and ensure calendar sync stability

---

6. Change & Incident Management

- Changes to the meeting system infrastructure must be reviewed with the Management Team.
- All incidents must be logged into the internal ITSM system JIRA and escalated by defined severity.

---

7. Compliance & Data Security

- All systems must comply with internal **data protection policies** and applicable regulations such as GDPR and PCI guidelines.
- Sensitive meeting data must be encrypted in transit and at rest.

These objectives apply to all critical systems listed in this SLA, including Integration APIs, Reporting Systems, Authentication Services, and Notification Services. RTO and RPO will be reviewed during the SLA review period and adjusted as needed based on business impact assessments.

- Recovery Point Objective (RPO): The maximum acceptable amount of data loss measured in time, defining the point to which data must be restored.
RPO: 15 minutes

- Recovery Time Objective (RTO): The maximum acceptable duration of time that services may be unavailable after an incident.
RTO: 4 hours

To support business continuity and ensure timely service restoration in the event of a disruption, the following recovery objectives are defined:

7.1 Recovery Objectives

8. SLA Violations & Remedies

- **Internal**: Reviewed in monthly operations meetings; potential impact on team KPIs.

- **AWS/Azure**: Service credits issued based on published SLA terms:
    - AWS SLA
    - Azure SLA

---

9. Review and Termination

- SLA is reviewed **biannually** or upon major service change.
- Termination requires a 30-day notice by either party.
