



BOHIOSYSTEM

• SERVICE LEVEL AGREEMENT • BOHIOSYSTEM

SLA · Cloud & Platform

Service levels, response times, and operational commitments for managed cloud platforms.

DOCUMENT

BS-SVC-05B

VERSION

1.0

DATE

August 1, 2026

PREPARED BY

BohioSystem

BohioSystem

bohiosystem.dev · Confidential

MEASURABLE COMMITMENTS

A service level agreement is only useful if it can be verified and carries consequences. This document defines both.

The values described here are our reference levels. The final agreement is signed per client and can be adjusted in either direction depending on the criticality of the platform and the contracted service window.

99.9%REFERENCE
AVAILABILITY**15 min**

CRITICAL RESPONSE

24/7

AVAILABLE WINDOW

Monthly

COMPLIANCE REPORT

01

Service levels

Three levels, depending on what the platform means to the business.

LEVEL	WINDOW	AVAILABILITY	TYPE OF PLATFORM
Essential	Mon–Fri, 8:00–18:00	99.5%	Internal systems whose downtime is disruptive but does not stop billing.
Advanced	Mon–Sun, 7:00–22:00	99.9%	Customer-facing platforms with extended business hours.
Critical	24/7/365	99.95%	Systems whose unavailability stops operations or revenue.

WHAT THOSE PERCENTAGES MEAN

A monthly 99.9% allows for **43 minutes** of downtime per month. A 99.95% allows just over 21 minutes. A 99.5% allows nearly three and a half hours. Choose the number based on what downtime costs, not on what sounds good.

02

Severity and response times

Severity is determined by business impact, not technical difficulty.

SEVERITY	DEFINITION	RESPONSE	RESOLUTION TARGET
S1 · Critical	Service down or unusable for all users. Data loss or an active security breach.	15 minutes	4 hours or a temporary workaround
S2 · High	Core function degraded or affecting a large group of users, with no viable workaround.	1 hour	8 business hours
S3 · Medium	Secondary function affected or an acceptable workaround exists.	4 business hours	3 business days
S4 · Low	Inquiry, minor enhancement, or cosmetic defect with no operational impact.	1 business day	Next planned cycle

03

What the managed service includes

Monitoring

- Availability and performance monitoring.
- Alerts with agreed thresholds.
- Proactive detection before users report an issue.
- Status dashboard accessible to the client.

Continuity

- Backups per the agreed policy.
- Periodic restore testing.
- Documented recovery plan.
- Annual recovery drill.

Operations

- Patching and updates.
- Certificate management and renewal.
- Scaling based on demand.
- Periodic capacity review.

Security

- Access and permissions review.
- Vulnerability analysis.
- Secrets management and rotation.
- Retained audit log.

04

Recovery objectives

Two numbers worth agreeing on before the incident, not during it.

OBJECTIVE	WHAT IT MEASURES	REFERENCE VALUES
RTO	Maximum acceptable time to return to service after a major outage.	Essential: 8 h · Advanced: 4 h · Critical: 1 h
RPO	Maximum amount of data acceptable to lose, measured in time.	Essential: 24 h · Advanced: 4 h · Critical: 15 min

THE QUESTION THAT DECIDES EVERYTHING

If the platform went down right now, how long could the business keep running, and how much data can it afford to lose? The answer to those two questions determines the service level and its cost.

05

Exclusions and client responsibilities

An honest agreement also states what it does not cover.

ITEM	TREATMENT
Maintenance windows	Planned and announced at least 72 hours in advance. Not counted as downtime.
Cloud provider failure	A regional outage at the provider is excluded from the calculation, unless the contracted design included cross-region redundancy.
Unauthorized changes	Modifications made by the client outside the agreed procedure suspend the commitment until the known state is restored.
Access and decisions	The client keeps access credentials current, responds to blocking questions, and designates a point of contact with decision-making authority during incidents.
Infrastructure costs	The cloud provider bill belongs to the client and is separate from the managed service. We optimize it; we do not absorb it.

06

Reporting and review

MONTHLY REPORT

Actual availability, incidents, response times, and consumption.

QUARTERLY REVIEW

Capacity, costs, risks, and improvement roadmap.

POST-MORTEM

For every S1 incident, with root cause and corrective actions.

Let's talk

NEXT STEP

Write to us and we'll schedule a working session at no cost to review your specific case.

CONTACT

contacto@bohiosystem.dev

WEB

bohiosystem.dev

DOCUMENT

BS-SVC-05B · v1.0