

Service Level Agreement

Last updated: 9 June 2026



1. SERVICE AVAILABILITY AND UPTIME SLA

1.1 UPTIME COMMITMENT

Maximum 3.6 hours unplanned downtime per 30-day month.

1.2 MEASUREMENT

Uptime measured from Opisense infrastructure perspective (EU infrastructure health checks), excluding scheduled maintenance windows (48-hour notice, max 4 hours/month) and events beyond control (Tier 1 cloud provider outages, internet backbone failures, DDoS attacks).

2. PERFORMANCE METRICS

2.1 RESPONSE TIME

Core platform API responds within: P95 < 500ms, P99 < 1000ms. Excludes AI sub-processor latency (OpenAI, Anthropic, ElevenLabs).

2.2 ERROR RATE

API error rate (5xx) maintained at <0.1% under normal load.

3. RECOVERY OBJECTIVES (GDPR ART. 32(2)(B))

3.1 OVERVIEW

Pursuant to GDPR Article 32(2)(b), Opisense has defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for critical services, ensuring rapid restoration of confidentiality, integrity, and availability of personal data.

3.2 RECOVERY TIME OBJECTIVE (RTO)

Details by service tier:

- **Critical Services (Chat, Document Processing, Voice Agents):** RTO = 4 hours - Must restore within 4 hours
- **Standard Services (Analytics, Reporting):** RTO = 8 hours
- **Best-Effort Services (Sandbox, Testing):** RTO = Best-effort

3.3 RECOVERY POINT OBJECTIVE (RPO)

In worst-case complete data center failure, Opisense restores data from backups no more than 1 hour prior to failure. Maximum 1 hour of transactional data loss.

3.4 RECOVERY MECHANISMS

RTO and RPO achieved through:

- **Multi-AZ Deployment:** Primary in Hetzner EU (Germany); automatic failover to secondary zone within 5 minutes
- **Database Replication:** Real-time replication across zones
- **Hourly Backups:** Automated snapshots every hour; encrypted, stored in separate region (eu-west-1 Ireland)
- **Backup Testing:** Quarterly restoration tests
- **API/Cache Redundancy:** Stateless API layers rapidly redeployable; Redis rebuilt from database in minutes

Service Level Agreement

Last updated: 9 June 2026



3.5 DISASTER RECOVERY TESTING SCHEDULE

Opisense conducts:

- **Quarterly Backup Restoration Test (Jan, Apr, Jul, Oct):** Full database restore in test environment; integrity validated; time measured. Results logged and provided on request.
- **Semi-Annual Failover Drill (Mar & Sep):** Planned failover from primary to secondary; services operational; latency increases slightly (<1 sec). RTO <4 hours confirmed.
- **Annual DR Plan Review (Dec):** Business Continuity Plan (ISMS-BCP-001) reviewed, updated, socialized.

3.6 REFERENCE DOCUMENTS

Detailed procedures documented in:

- **ISMS-BCP-001:** Business Continuity Plan - detection, response, recovery, communication
- **ISMS-DR-001:** Disaster Recovery Plan - technical runbooks for failover, restore, validation
- **ISMS-IR-001:** Incident Response Plan - roles, escalation, coordination

Available to customers under NDA upon request.

4. DISASTER RECOVERY AND BUSINESS CONTINUITY

4.1 DISASTER SCENARIOS COVERED

Plan addresses:

- Infrastructure Failure - Hetzner zone down, failover to secondary
- Data Center Outage - full Hetzner primary region down, failover to secondary region
- Data Corruption - restore from hourly backup
- Ransomware/Malicious Activity - isolation, recovery from clean backups, investigation
- Third-Party Dependency Failure - fallback to alternates or service degradation

4.2 INCIDENT CLASSIFICATION

- **Critical:** Completely unavailable; RTO clock starts. Page on-call; executive notification; begin failover. Target: <15 min mitigation, <4 hrs recovery.
- **Major:** >50% users affected; RTO applies. Notify customer; escalate to engineering. Target: <1 hr investigation, <4 hrs recovery.
- **Minor:** <50% affected; best-effort. Standard support process.

5. MONITORING AND REPORTING

5.1 CONTINUOUS MONITORING

Monitored: infrastructure health (CPU, memory, disk, network), database performance, API health, third-party status, security indicators. Automated alerting is reviewed during critical hours (business hours for Standard tier; 24/7 for Enterprise tier).

5.2 MONTHLY UPTIME REPORT

Published by 5th of following month with: actual uptime %, incidents (date, duration, root cause, impact, resolution), downtime breakdown (planned vs. emergency), SLA compliance, credits applied. Available via customer dashboard or request.

Service Level Agreement

Last updated: 9 June 2026



5.3 INCIDENT COMMUNICATION

During incidents: Customer alert within 15 minutes, status page updated every 30 minutes (opisense.com/status), RCA within 48 hours, post-incident review within 5 business days.

6. SERVICE CREDITS AND REMEDIES

6.1 UPTIME SHORTFALL CREDITS

If monthly uptime <99.5%:

- 99.0-99.4%: 5% credit
- 98.0-98.9%: 10% credit
- 95.0-97.9%: 25% credit
- <95.0%: 30% credit

6.2 CREDIT REDEMPTION

Credits applied automatically to next invoice. No rollover; unused credits forfeited at year-end.

6.3 EXCLUSIVE REMEDY

Service credits are the exclusive remedy for SLA shortfalls caused by infrastructure or platform performance issues within Opisense's control and not resulting from gross negligence or willful misconduct. Service credits do not apply to outages caused by Customer's breach of AUP or misconfiguration. If Opisense fails to meet SLA targets for more than 2 months in any 12-month period, Customer may terminate the Service without penalty.

7. EXCLUSIONS

7.1 EVENTS NOT COVERED BY SLA

SLA not applicable to: scheduled maintenance (48+ notice), internet backbone/DNS failures, DDoS/ malicious interference, failures or unavailability of third-party sub-processors beyond Opisense control, customer misconfiguration/AUP breach, force majeure (natural disaster, war, government action).

8. CUSTOMER SUPPORT

8.1 SUPPORT TIERS

- **Free/Trial:** Community forum + email (24-48 hr SLA)
- **Professional:** Email/chat (4-8 hr SLA), phone business hours
- **Enterprise:** Dedicated engineer, 1-4 hr SLA, 24/7 critical, quarterly review

8.2 SUPPORT CONTACT

- Standard: contact@opisense.com
- Security/Incident: security@opisense.com (within 1 hour)
- Critical Outage: [dedicated line — number to be published at opisense.com/support]

SLA effective: 2026-04-06. Opisense may update with 30 days notice. RTO/RPO and testing schedule changes must be communicated to customers.