

SUPPORT SPECIFICATION

This Support Specification defines the service commitments, availability guarantees, support levels, and remedies available to Customer for the Platform hosted on Amazon Web Services (AWS) infrastructure.

1. SERVICE AVAILABILITY COMMITMENT

1.1 Uptime Guarantee

The Supplier commits to 99.9% Monthly Uptime for the Platform. Monthly Uptime is calculated as follows:

$$\text{Monthly Uptime \%} = (\text{Total Minutes in Month} - \text{Downtime Minutes}) / \text{Total Minutes in Month} \times 100$$

1.2 Exclusions from Downtime

The following are excluded from downtime calculations:

- **Scheduled Maintenance:** Planned maintenance windows notified at least forty-eight (48) hours in advance, conducted outside Customer's primary business hours, not exceeding four (4) hours per month.
- **Emergency Maintenance:** Critical security patches or infrastructure updates required to maintain platform security or stability, with maximum two (2) hours advance notice where possible.
- **Customer-Caused Downtime:** Service interruptions resulting from Customer's equipment, network, software, or misuse of the Platform.
- **Force Majeure Events:** Events beyond the Supplier's reasonable control including natural disasters, acts of government, telecommunications failures, cyberattacks targeting AWS infrastructure, or regional AWS service disruptions.
- **Third-Party Service Failures:** Failures of third-party services not under the Supplier's direct control, including internet service providers, DNS services, or Customer's own network connectivity.
- **Beta or Preview Features:** Any Platform features designated as beta, preview, or experimental

1.3 AWS Infrastructure

The Platform is hosted on Amazon Web Services (AWS) infrastructure across multiple availability zones to ensure high availability and fault tolerance. The Supplier leverages AWS's enterprise-grade infrastructure, including:

- Multi-AZ deployment architecture for redundancy;
- Automated failover and load balancing;
- AWS-native monitoring and alerting systems; and
- Geographic redundancy across AWS regions where applicable.

2. PERFORMANCE STANDARDS

2.1 Response Time Targets

The Supplier aims to achieve the following response time targets for the Platform under normal operating conditions:

Operation Type	Target Response Time	Measurement
Page Load Time	< 3 seconds	95th percentile
API Response Time	< 500 milliseconds	95th percentile
Data Synchronization	< 5 minutes	Average

Note: Response times may vary based on Customer's network conditions, geographic location, and data volume. These targets apply to AWS-hosted infrastructure under normal load conditions.

3. Incident Response and Support

3.1 Support Availability

The Supplier provides 24/7/365 technical support for Critical and High Priority incidents. Standard support is available during business hours (09:00-17:00 GMT, Monday-Friday, excluding UK bank holidays).

3.2 Incident Classification and Response Times

Incidents are classified based on severity and business impact:

Priority	Definition	Initial Response	Resolution Target
Critical	Complete service outage, security breach, or data loss affecting production	1 hour	4 hours (workaround) 48 hours (resolution)
High	Major functionality impaired, significant performance degradation	4 hours	7 business days
Medium	Minor functionality affected, workaround available	1 business day	14 business days
Low	Cosmetic issues, minor bugs, feature requests	2 business days	Next release cycle

3.3 Post-Incident Reporting

For Critical incidents, the Supplier will provide a post-incident report within seven (7) business days of resolution, including:

- Incident timeline and detection method;
- Root cause analysis;
- Impact assessment;
- Remediation actions taken; and
- Preventive measures implemented

4. SECURITY AND COMPLIANCE

4.1 Vulnerability Management

The Supplier follows industry-leading vulnerability management practices:

- **Critical Vulnerabilities:** Patched within forty-eight (48) hours of discovery
- **High-Priority Vulnerabilities:** Addressed within seven (7) days
- **Medium-Priority Vulnerabilities:** Resolved within fourteen (14) days
- **Low-Priority Vulnerabilities:** Addressed on best-effort basis

The Supplier employs automated vulnerability scanning tools including, but not limited to, SonarQube, GoSec, and AWS Inspector. Critical or high-priority vulnerability solutions will not be deployed to production without resolution or documented exception with compensating controls.

4.2 Security Monitoring

The Supplier maintains continuous security monitoring using tools including, but not limited to, DataDog and AWS-native services (CloudWatch, GuardDuty, Security Hub) to detect and respond to security threats in real-time. Security alerts are triaged 24/7, with Critical security incidents escalated immediately.

4.3 Compliance Certifications

The Supplier is committed to obtaining SOC 2 Type II certification (annual audit) and aims to achieve this outcome (using commercially reasonable efforts) before the end of 2027.

5. DATA PROTECTION AND BUSINESS CONTINUITY

5.1 Data Backup

All Customer Data is automatically backed up using AWS backup services with the following parameters:

- **Backup Frequency:** Daily automated backups;
- **Backup Retention:** thirty (30) days for standard backups, ninety (90) days for compliance backups;
- **Backup Encryption:** AES-256 encryption at rest; and
- **Geographic Redundancy:** Cross-region replication to secondary AWS region.

6. MONITORING AND REPORTING

6.1 Platform Monitoring

The Supplier maintains continuous monitoring of platform health, performance, and security using tools including, without limitation, DataDog, AWS CloudWatch, and custom monitoring solutions. Automated alerts ensure rapid incident detection and response.

6.2 Customer Reporting

The Supplier provides the following reports to Customer upon request:

- **Monthly Uptime Report:** Actual uptime percentage, downtime incidents, and service credit calculations if applicable;
- **Quarterly Performance Report:** Response time metrics, incident statistics, and support ticket resolution data; and
- **Annual Security Report:** Security incidents, vulnerability management summary, and compliance certification status.

7. SUPPORT SPECIFICATION REVIEW AND MODIFICATION

The Supplier reserves the right to modify this Support Specification with sixty (60) days written notice to Customer. If in the Customer's reasonable opinion, material changes to the Support Specification adversely affect the Customer, Customer may terminate the Agreement by providing written notice to the Supplier within thirty (30) days of receipt of the Supplier's written notice. This Support Specification is reviewed annually and updated to reflect evolving service capabilities, industry standards, and customer requirements.

8. CONTACT INFORMATION

For support requests, incident reporting, or Service Level related inquiries:

- **Technical Support:** support@hybird.ai
- **Security Incidents:** security@hybird.ai