



SERVICE LEVEL AGREEMENT (SLA)

AGen SaaS Platform

Contents

SERVICE LEVEL AGREEMENT (SLA) for AGen SaaS Platform provided by ALC-TECH (M) SDN BHD	3
1. Definitions.....	4
2. Scope of Services Covered	5
3. Service Levels.....	6
3.1 Availability / Uptime	6
3.2 Support Response & Resolution Times	6
3.3 Bug Fixes & Updates	6
3.4 API Performance	7
3.5 Data Backup & Recovery	7
3.6 Scheduled Maintenance.....	7
3.7 Security, OS Upgrades, Patching & Major Bug Fixes	7
3.8 User Access Management and Audit Logging	8
3.8.1 User Access Management	8
3.8.2 Audit Logging.....	8
3.9 Data Backup and Disaster Recovery	9
3.9.1 Data Backup.....	9
3.9.2 Disaster Recovery	9
3.9.3 Customer Responsibilities.....	10
3.9.4 Limitations	10
3.10 Service Recovery – Web Server Unavailability	10
3.11 Monitoring and Alerting	11
3.11.1 Monitoring.....	11
3.11.2 Alerting.....	12
3.11.3 Customer Notification	12
3.11.4 Limitations	12
4. Measurement, Reporting & Review.....	13
5. Remedies	13
6. Exclusions	13



7. Customer Responsibilities	14
8. Support Channels & Hours	14
9. Term & Changes.....	14
10. General.....	14
Signed for and on behalf of:	15
ALC-TECH (M) SDN BHD	15
Customer	15

SERVICE LEVEL AGREEMENT (SLA) for AGen SaaS Platform provided by ALC-TECH (M) SDN BHD

This Service Level Agreement (“SLA”) forms part of the agreement between:

Provider: ALC-TECH (M) SDN BHD (Company No. [610609-M]) [No:30-1, Jalan 6/62A, Bandar Manjalara, 52200 Kepong, Kuala Lumpur, Malaysia.] (“Provider”, “we”, “us” or “our”)

This SLA sets out the service levels that apply to the SaaS product (the “Service”) provided by the agen.mobi domain.



1. Definitions

Term	Meaning
Availability / Uptime	The percentage of time the Service is accessible and usable by authorized users during the Measurement Period, excluding Scheduled Maintenance and Exclusions.
Business Hours	Monday to Friday, 9:00 a.m. to 5:00 p.m. Malaysia Time (MYT), excluding Malaysian public holidays.
Critical Incident	Complete unavailability of the Service or a major function that prevents many users from performing core business operations.
High Incident	Significant degradation or failure of a major feature that materially impacts Customer's operations, but a workaround may exist.
Medium Incident	Partial loss of functionality or performance issue that affects some users or non-core features, with a reasonable workaround available.
Low Incident	Minor issues, cosmetic defects, or general enquiry that do not materially affect operations.
Measurement Period	Each calendar month.
Scheduled Maintenance	Planned maintenance windows notified in advance.
Service	The hosted SaaS software platform provided by the Provider, including any related APIs and supported modules.

2. Scope of Services Covered

This SLA covers the following:

- Hosted availability / uptime of the Service
- Support response and resolution / workaround times
- Bug fixes and updates
- API performance (availability and basic responsiveness)
- Data backup and recovery

This SLA does **not** cover third-party services, Customer's own infrastructure, internet connectivity, or any custom developments outside the standard Service.



3. Service Levels

3.1 Availability / Uptime

Metric	Target
Uptime Percentage	99%

3.2 Support Response & Resolution Times

Support is provided during **Business Hours** only via email, chat and telephone.

Severity	Response Time (Business Hours)	Resolution / Workaround Target
Critical	1 Business Day	1 Business Day
High	2 Business Day	2 Business Day
Medium	3 Business Day	3 Business Day
Low	3 Business Day	Best effort (target 5 Business Days)

Notes:

- “Response Time” means the time from receipt of a properly submitted support ticket until the provider first acknowledges and begins investigation.
- “Resolution / Workaround” means either a permanent fix or a temporary workaround that restores usable functionality.
- Targets for Critical and High incidents apply only when the issue is confirmed to be within the agen.mobi control.

3.3 Bug Fixes & Updates

- Critical and High severity bugs will be prioritized according to the table above.
- Non-urgent bug fixes and product updates will be released on a regular cadence as determined by the AGen team.
- Security-related updates will be applied as soon as reasonably practicable.



3.4 API Performance

- AGen team will use commercially reasonable efforts to maintain API availability consistent with the overall Uptime target.
- AGen team does not guarantee specific latency or throughput figures unless separately agreed in writing.

3.5 Data Backup & Recovery

- Production data is backed up daily.
- Backup retention: minimum 30 days.
- In the event of data loss caused by the agen.mobi, the AGen team will restore data from the most recent available backup as soon as reasonably practicable.
- Customer is responsible for maintaining their own copies of critical data where required for business continuity.

3.6 Scheduled Maintenance

- The Provider may perform Scheduled Maintenance up to **two (2) times per calendar year**.
- Each maintenance window will not exceed 8 hours unless otherwise notified.
- AGen team will provide at least **7 days' prior written notice** (email or in-app notification) of Scheduled Maintenance, except in urgent security or stability cases where shorter notice may be given.

3.7 Security, OS Upgrades, Patching & Major Bug Fixes

AGen team are responsible for the maintenance and security of the underlying infrastructure that hosts the Service. In particular:

1. **Operating System Upgrades** Apply Necessary Operating System upgrades to the servers hosting the Service in a timely manner, taking into account stability, security, and compatibility with the Service.
2. **Security Patching** Apply critical and high-severity security patches to the Operating System, middleware, and relevant platform components within a reasonable timeframe after they become available and have been tested for compatibility.



3. **Major Bug Fixes** Priorities and implement fixes for major bugs that affect the security, stability, or core functionality of the Service, in accordance with the severity and response times set out in this SLA.
4. **Malware and Ransomware Protection** Implement and maintain industry-standard security measures designed to protect the Service against malware, ransomware, and similar threats. These measures include, but are not limited to, regular security updates, access controls, monitoring, and backup practices.
5. **Regulatory Compliance Support** Maintain the hosted environment in a manner that supports the Provider's compliance with applicable information security and data protection standards. The Provider does not guarantee that the Customer's use of the Service will meet any specific regulatory or compliance requirements applicable to the Customer's business. The Customer remains solely responsible for his own regulatory compliance.

3.8 User Access Management and Audit Logging

3.8.1 User Access Management

- AGen team maintain appropriate access controls for its own personnel and systems that support the Service. Access to production systems is restricted on the least privilege basis and is subject to regular review.
- AGen team provides features that allow the Customer to manage user accounts, roles, and permissions for its own authorized users. The Customer is solely responsible for:
 - Creating, modifying, and deactivating user accounts within the Service
 - Assigning appropriate roles and permissions
 - Ensuring that only authorized individuals have access
 - Promptly removing access for users who no longer require it
- The Provider will not create, modify, or delete Customer user accounts except at the Customer's written request or as required for support, security, or legal reasons.

3.8.2 Audit Logging

- The Provider maintains audit logs of relevant system and security-related events within the Service and its supporting infrastructure. These logs typically include (where applicable):



- User login and logout events
- Changes to user accounts and permissions
- Significant administrative actions
- Selected security-relevant system events
- Upon reasonable written request, and subject to the Provider's security and confidentiality policies, the Provider will make relevant audit log information available to the Customer to support investigations or compliance needs.
- The Customer is responsible for reviewing and monitoring activity within his own user accounts and for any logging features made available to it inside the application.

Limitations AGen team does not guarantee that every possible action within the Service will be logged, nor that logs will be sufficient on their own to meet all of the Customer's regulatory or internal audit requirements. The Customer remains responsible for determining whether the available logging meets its specific compliance needs.

3.9 Data Backup and Disaster Recovery

3.9.1 Data Backup

- AGen team performs regular backups of the Customer's production data stored within the Service.
- **Backup Frequency:** Full backups are performed **daily**.
- **Backup Retention:** Backups are retained for a minimum of **30 days**.
- Backups are stored in a secure location that is logically or physically separated from the primary production environment.

3.9.2 Disaster Recovery

- The Provider maintains disaster recovery arrangements designed to restore the Service in the event of a significant incident affecting the primary infrastructure.
- In the event of a disaster that causes prolonged unavailability of the Service, the Provider will use commercially reasonable efforts to restore the Service and recover Customer data from the most recent available backup.



Recovery Objectives (Targets):

Objective	Target
Recovery Point Objective (RPO)	Maximum 24 hours of data loss
Recovery Time Objective (RTO)	Service restoration within 48 hours (target)

Note: These are target objectives, not absolute guarantees. Actual recovery time may vary depending on the nature and severity of the incident.

3.9.3 Customer Responsibilities

- The Customer is responsible for maintaining its own copies of critical data where required for business continuity or regulatory purposes.
- The Customer should regularly export or download important data if additional local copies are needed.

3.9.4 Limitations

- The Provider does not guarantee that data recovery will be possible in every scenario (for example, in cases of extreme corruption, encryption by ransomware before backup, or force majeure events).
- Restoration from backup may result in the loss of data entered after the last successful backup (up to the RPO).
- Disaster recovery commitments apply only to the Service hosted by the AGen team and do not cover the Customer's own systems, networks, or devices.

3.10 Service Recovery – Web Server Unavailability

If the web server hosting the Service becomes unavailable or unreachable (i.e. the Service cannot be accessed by authorized users due to a failure on the Provider's side), the following response and recovery commitments apply:

Stage	Target Timeframe	Description
Detection & Response	Within 1 Business days	AGen team will acknowledge the incident and begin investigation after it is detected by monitoring systems or reported by the Customer.
Service Restoration (Target)	Within 3 business day	AGen team will use commercially reasonable efforts to restore the web server and make the Service available again.
Major / Disaster-level Outage	Within 2 Business days	In the event of a significant infrastructure failure requiring disaster recovery procedures, the target restoration time is 48 hours from declaration of the disaster.

Classification Unavailability of the web server that prevents the majority of users from accessing the Service will normally be classified as a **Critical Incident**.

Conditions

- These timeframes apply only during **Business Hours** (Monday–Friday, 9:00 a.m. – 5:00 p.m. Malaysia Time, excluding public holidays), unless otherwise agreed.
- Timeframes start from the point the Provider becomes aware of the incident (via monitoring or Customer notification).
- Restoration targets exclude issues caused by Customer-side problems, third-party services, internet connectivity, or force majeure events.
- The Provider will keep the Customer reasonably informed of progress during the recovery process.

Reporting Upon request, the Provider will provide a brief incident summary explaining the cause (where known) and the actions taken to restore service.

3.11 Monitoring and Alerting

3.11.1 Monitoring

The Provider continuously monitors the servers and key components that support the Service. Monitoring typically covers:

- Server availability and uptime



- System resource utilization (CPU, memory, disk, etc.)
- Application and web server health
- Critical services and processes
- Basic security-related events (where applicable)

Monitoring is performed using automated tools on a 24 × 7 basis.

3.11.2 Alerting

- Automated alerts are generated when predefined thresholds are breached or when the Service becomes unavailable.
- Alerts are sent to the AGen team so that investigation and response can begin in accordance with the severity and response times defined in this SLA.
- Critical alerts related to Service unavailability are treated as **Critical Incidents**.

3.11.3 Customer Notification

- In the event of a confirmed incident that materially affects the availability or performance of the Service, the Provider will notify the Customer's designated contact(s) within a reasonable time after the incident has been verified.
- Updates will be provided at reasonable intervals until the Service is restored.

3.11.4 Limitations

- Monitoring and alerting are designed to detect material issues affecting the Service. AGen team do not guarantee that every possible anomaly or early-stage problem will be detected immediately.
- AGen team's monitoring focuses on the infrastructure and application components under its control. It does not monitor the Customer's internal networks, devices, or third-party systems.
- Alert response times follow the Business Hours and severity levels stated in this SLA, unless otherwise agreed in writing.



4. Measurement, Reporting & Review

- Uptime and support performance will be measured monthly.
- Upon written request, AGen team will provide a daily data collected report showing actual service running.
- The parties may review this SLA annually or upon mutual written agreement.

5. Remedies

If the AGen team fails to meet the Uptime or support targets in any Measurement Period, AGen team will:

1. Investigate the cause;
2. Provide a written explanation to the Customer upon request; and
3. Take reasonable corrective actions.

There are no service credits, financial penalties, or refunds under this SLA. Persistent or material failure to meet the service levels may be addressed under the termination provisions of the main agreement between the parties.

6. Exclusions

The following are excluded from Uptime calculations and service level commitments:

- Scheduled Maintenance
- Issues caused by Customer's acts or omissions, including misconfiguration, unauthorized use, or failure to follow documentation
- Force majeure events (including natural disasters, war, terrorism, internet backbone failures, power outages outside the Provider's control, or government actions)
- Failures of third-party services or infrastructure not under the Provider's direct control
- Beta, trial, or preview features
- Suspension of the Service due to Customer's non-payment or breach of the main agreement



7. Customer Responsibilities

The Customer shall:

- Use the Service in accordance with the documentation and acceptable use policy
- Provide timely and accurate information when raising support tickets
- Maintain appropriate access controls and security on its side
- Ensure its users are properly trained
- Promptly apply any required configuration changes or updates notified by the Provider

8. Support Channels & Hours

Channel	Availability
Email	Business Hours
Chat	Business Hours
Telephone	Business Hours

Support requests received outside Business Hours will be logged and addressed on the next Business Day according to the severity table.

9. Term & Changes

This SLA remains in effect for the duration of the main agreement between the parties. AGen team may update this SLA from time to time by giving reasonable prior notice. Material adverse changes will be communicated at least 30 days in advance.

10. General

This SLA is governed by the laws of Malaysia. It forms part of, and is subject to, the main Master Service Agreement / Terms of Service between the parties. In the event of conflict, the main agreement prevails unless expressly stated otherwise.



Signed for and on behalf of:

ALC-TECH (M) SDN BHD

Name: _____

Title: _____

Date: _____

Signature: _____

Customer

Name: _____

Title: _____

Date: _____

Signature: _____

