

[_> SERVICE_COMMITMENTS](#)

Service Levels & Support Policy

Operational standards for Managed WordPress Hosting

Field	Value
Provider	ANTIHOST S.R.L. / Antihost
Product scope	Managed WordPress Hosting
Version	1.0 - Draft for review
Effective date	To be confirmed before publication
Last updated	30 June 2026

Current operating standard

This policy reflects the current operational standards of Antihost. As the platform evolves, service processes and response objectives may improve. Material changes will be communicated in advance and will not reduce the level of service for existing customers without prior notice.

This document is written as a customer-facing operational policy, not as a marketing page. It defines what Antihost commits to, what is excluded, and where responsibility is shared.

Contents

1. Purpose and status
2. Quick reference
3. Product scope
4. Availability commitment
5. Support channels and support hours
6. Incident priority matrix
7. Response objectives
8. Monitoring and operational checks
9. Maintenance policy
10. Backups and recovery
11. WordPress updates
12. Migration policy
13. SSL certificates
14. Responsibility matrix
15. Service credits and compensation
16. Exclusions
17. Definitions
18. Change management
19. Contact information
20. Version history

1. Purpose and status

This Service Levels & Support Policy defines Antihost's availability commitments, response objectives, maintenance rules, backup and recovery approach, support channels, and shared operational responsibilities for Managed WordPress Hosting customers.

The purpose is to make service expectations explicit before a customer relies on Antihost for a production WordPress project.

Legal relationship

This policy should be read together with Antihost Terms & Conditions, Refund Policy, Privacy Policy, and any customer-specific agreement. If a signed customer agreement defines a different service level, the signed agreement takes priority for that customer.

2. Quick reference

Area	Commitment	Notes
Availability	99.99% monthly platform availability target	Applies to Antihost platform infrastructure for Managed WordPress Hosting.
Critical incidents	Initial response within 30 minutes	Applies 24/7 when a verified critical infrastructure incident affects production availability.
Non-critical requests	Initial response within 1 business hour	Applies during support hours: 09:00-19:00 Europe/Kyiv, Monday-Friday.
Planned maintenance	Communicated at least 72 hours in advance	Scheduled during low-impact windows whenever reasonably possible.
Backups	Daily internal backups retained for 30 days	Customer-created manual backups can be restored from the panel; internal backups are restored on request.
Credits	Reviewed individually	Hosting credits may be issued to the customer credit balance at Antihost's discretion after verified service disruption.

3. Product scope

This policy applies to Managed WordPress Hosting plans operated by Antihost.

4. Availability commitment

Antihost targets 99.99% monthly availability for the platform infrastructure used to operate Managed WordPress Hosting.

Availability means the ability to access the Antihost platform infrastructure and hosted WordPress instances over the public Internet when the issue is caused by Antihost-controlled infrastructure.

Metric	Commitment	Measurement logic
Platform availability	99.99% monthly	Measured against Antihost-controlled infrastructure and monitored service availability.
Scheduled maintenance	Excluded from availability calculation	Applies only when announced at least 72 hours in advance.
Customer application failures	Excluded	Plugin errors, theme bugs, customer code, content changes, or configuration mistakes are not counted as platform downtime.

How to read 99.99%

99.99% monthly availability leaves approximately 4 minutes and 23 seconds of unplanned downtime in a 30-day month. This is a platform infrastructure objective, not a guarantee that every WordPress application will be free from application-level errors.

5. Support channels and support hours

Customers can contact Antihost support through the following channels:

- Support tickets through the customer panel or support portal.
- Email support.
- Chatwoot live chat or asynchronous chat on the website or customer interface.
- Messenger-based support may be reviewed on request for Agency and Business plans, depending on customer needs and operational feasibility.

Request type	Coverage
Critical infrastructure incidents	24/7 initial response coverage.

Request type	Coverage
Major and general requests	09:00-19:00 Europe/Kyiv, Monday-Friday.
Messenger-based support	Optional, reviewed individually for Agency and Business plans.

Response time means the first meaningful response from Antihost: acknowledgement, initial assessment, request for missing details, or next operational step. Response time is not the same as resolution time.

6. Incident priority matrix

Antihost uses three priority levels to keep support expectations clear.

Priority	Definition and examples	Response objective
Critical	Production WordPress site or platform function is unavailable due to a verified Antihost infrastructure issue. Examples: server availability outage, platform-wide incident, provisioning or DNS automation failure blocking launch.	24/7 initial response within 30 minutes.
Major	Service is degraded but not fully unavailable. Examples: abnormal resource behavior, backup restore request, SSL issuance issue, instance provisioning problem that does not affect all customers.	Initial response within 1 business hour during support hours.
General	Questions, plan changes, migration scheduling, configuration clarification, documentation requests, minor UI or panel issues.	Initial response within 1 business hour during support hours.

7. Response objectives

Response objectives are designed around operational impact, not the number of tickets submitted.

Priority	Initial response	Coverage	Expected first action
Critical	Within 30 minutes	24/7	Initial investigation starts. Customer receives acknowledgement and next operational step.
Major	Within 1 business hour	09:00-19:00 Europe/Kyiv, Monday-Friday	Issue is reviewed and routed to the appropriate operational owner.
General	Within 1 business hour	09:00-19:00 Europe/Kyiv, Monday-Friday	Customer receives answer, clarification request, or next step.

Current stage of operations

These response objectives reflect Antihost's current operating model. As the support team expands, Antihost may improve coverage and response objectives. Any material changes will be communicated in advance.

8. Monitoring and operational checks

Antihost monitors platform-level signals and automated workflows to detect infrastructure issues before they affect customers whenever possible.

Monitored area	What Antihost checks
Server availability	Infrastructure-level health checks for servers and core service availability.
Instance creation	Monitoring and automated tests for WordPress instance provisioning.
DNS record automation	Monitoring and automated tests for DNS record creation and related provisioning workflows.
Platform workflows	Automated tests and operational checks for flows that can be measured and tested reliably.
Resource behavior	Monitoring of relevant resource usage signals where available, including capacity and abnormal behavior.

Monitoring covers Antihost-controlled infrastructure and platform workflows. It does not replace customer-side monitoring of application-specific behavior, business transactions, third-party integrations, or custom WordPress logic.

9. Maintenance policy

Maintenance is part of keeping the platform stable. Antihost separates planned maintenance from emergency maintenance.

Type	Policy
Planned maintenance	Communicated at least 72 hours in advance. Scheduled during periods of lowest expected impact whenever reasonably possible. Planned maintenance announced in advance is excluded from the availability calculation.
Emergency maintenance	May be performed with shorter notice when required to protect platform stability, security, data integrity, or customer availability. Antihost communicates as early as reasonably possible.
Customer impact	When maintenance is expected to affect availability or performance, Antihost provides the expected scope, timing, and customer impact where possible.

10. Backups and recovery

Antihost maintains internal backups for Managed WordPress Hosting environments and provides customer-facing manual backup controls where available.

Area	Policy
Internal daily backups	Created daily and retained for 30 days.
Internal backup restore	Performed by Antihost on request. Restore time depends on site size, backup size, and incident context.
Manual backups	Customer-created manual backups can be restored by the customer from the panel when the backup was created through the available panel controls.
Restore responsibility	Antihost can restore infrastructure-level backups. The customer is responsible for validating the application after restore,

Area	Policy
	including plugins, theme behavior, forms, checkout, and third-party integrations.
Archival storage	Backups are operational recovery tools, not long-term compliance archives. Customers should keep their own independent copies when required by internal policy or regulation.

11. WordPress updates

Antihost does not automatically update WordPress core, plugins, or themes by default.

This is intentional. Automatic WordPress updates can introduce compatibility issues in production environments. Antihost provides one-click update tools while leaving deployment timing under the customer's control.

- Customers decide when to update WordPress core, plugins, and themes.
- Customers can use panel tools to initiate updates when ready.
- Antihost may recommend updates for security or stability reasons.
- Platform-level security updates may be applied by Antihost when required to protect infrastructure integrity.

Recommended update workflow

For business-critical sites, Antihost recommends creating or verifying a backup, testing risky updates in staging where available, and updating during a low-traffic window.

12. Migration policy

Migration assistance is included with all Managed WordPress Hosting plans, subject to reasonable technical scope.

For large or complex WordPress projects, migration may require individual assessment before the site can be accepted into a standard plan.

Migration area	Policy
Included migration	Standard WordPress site migration from another hosting provider to Antihost.
Complex migration	Large databases, heavy WooCommerce sites, multisite setups, custom server dependencies, unusual plugin stacks, or high-risk production systems may require higher-tier hosting or a custom quote.

Migration area	Policy
DNS switch	Antihost can assist with DNS switch planning. Propagation timing depends on DNS settings and third-party systems outside Antihost control.
Customer validation	After migration, the customer is responsible for confirming that application behavior, checkout, forms, integrations, and content are correct.

13. SSL certificates

Antihost provides Let's Encrypt SSL certificates for Managed WordPress Hosting environments and handles automatic renewal where domain configuration allows it.

- SSL issuance depends on correct domain and DNS configuration.
- If the domain is not pointed correctly, SSL issuance or renewal may fail until DNS is corrected.
- Third-party rate limits or external DNS failures are outside Antihost control.

14. Responsibility matrix

Operational stability depends on defined boundaries. Antihost manages the platform layer; the customer controls the application layer.

Area	Owner	Notes
Infrastructure availability	Antihost	Server, hosting environment, core platform infrastructure.
Network and host node	Antihost	Network connectivity and host-level operation under Antihost control.
WordPress application code	Customer	Custom code, application logic, custom functions.
WordPress content	Customer	Pages, posts, media, customer data, content changes.
Plugins and themes	Customer	Selection, licensing, compatibility, behavior after updates.
Daily internal backups	Antihost	Creation and retention of platform backups according to this policy.

Area	Owner	Notes
Manual backups	Shared	Customer can create and restore panel-based manual backups; Antihost maintains available backup tooling.
SSL automation	Antihost	Certificate issuance and renewal when DNS/domain configuration is valid.
DNS configuration	Shared	Antihost can automate or assist; customer must provide correct domain ownership/access and approve changes when required.
Third-party services	Customer	Payment gateways, CRM, email providers, APIs, analytics, external plugins, CDN settings outside Antihost control.
Security of user accounts	Customer	Passwords, MFA where available, account access, safe credential handling.
Incident communication	Shared	Antihost investigates infrastructure; customer provides accurate context, affected URLs, timestamps, and reproduction steps.

15. Service credits and compensation

Antihost does not provide automatic cash refunds for SLA-related disruptions.

After a verified Antihost-caused service disruption, hosting credits may be issued at Antihost's discretion after individual review.

- Credits are applied to the customer's Antihost credit balance.
- Credits can be used toward future Antihost invoices.
- Credits are not paid out as cash unless required by law or a separate written agreement.
- Credit eligibility depends on verified impact, cause, duration, customer plan, and whether the disruption was caused by Antihost-controlled infrastructure.

Why credits are reviewed individually

Infrastructure incidents vary by cause and customer impact. A case-by-case review prevents automatic compensation for issues outside Antihost control, such as customer application errors or third-party outages.

16. Exclusions

The following events are excluded from Antihost availability calculations and service credit review unless a separate written agreement states otherwise:

- Planned maintenance announced at least 72 hours in advance.
- Emergency maintenance required to protect security, stability, data integrity, or availability.
- Customer-side WordPress issues, including plugin conflicts, theme errors, custom code, corrupted content, or misconfiguration.
- Customer-initiated changes, including DNS changes, application updates, password changes, or deleted files.
- Third-party failures, including registrars, DNS providers, payment systems, email services, APIs, analytics tools, CDNs outside Antihost control, or customer Internet provider issues.
- DDoS attacks or abusive traffic beyond available mitigation capacity.
- Suspension or limitation of service due to abuse, policy violation, non-payment, legal requirement, or security risk.
- Force majeure events, including natural disasters, war, civil unrest, government action, global network incidents, or supplier failures outside reasonable control.

17. Definitions

Term	Definition
Availability	The ability to access Antihost-controlled platform infrastructure and hosted WordPress instances over the public Internet.
Critical incident	A verified infrastructure-level incident that makes a production service unavailable or blocks a key platform function.
Initial response	The first meaningful support response from Antihost: acknowledgement, assessment, request for data, or next operational step.
Resolution time	The time required to fully fix, restore, work around, or close an issue. Resolution time is not guaranteed by the response objectives in this policy.

Term	Definition
Maintenance	Planned or emergency work required to keep the platform secure, stable, and operational.
Business hour	An hour within 09:00-19:00 Europe/Kyiv, Monday-Friday, excluding public holidays unless otherwise stated.

18. Change management

This policy is expected to evolve as Antihost expands support capacity, improves platform automation, and matures its operational processes.

Material changes will be communicated in advance. Antihost will not reduce the service level for existing customers without prior notice. Improvements, such as faster response objectives or broader support coverage, may be introduced without waiting for a new contract cycle.

Living policy

This is a living operational policy. Its purpose is to document how Antihost works now and to make future improvements visible and traceable.

19. Contact information

Primary support channels are provided inside the Antihost customer panel and on the Antihost website.

Channel	Use
Support ticket	Best for account-specific issues, incidents, backups, migrations, and technical requests.
Email	Best for general support and follow-up communication.
Chatwoot chat	Best for quick questions, triage, and routing to the correct support path.
Messenger-based support	Reviewed individually for Agency and Business plans when operationally justified.

Customers reporting an incident should include: affected domain, affected URLs, time of first impact, screenshots or error messages, recent changes, and steps to reproduce where possible.

20. Version history

Version	Date	Status	Notes
1.0	30 June 2026	Draft for review	Initial customer-facing Service Levels & Support Policy for Managed WordPress Hosting.