Terms of Service & Acceptable Use Policy (AUP)

ALTIUS HOST LLC | Last Updated: November 12, 2026

1. Introduction

Welcome to ALTIUS HOST LLC ("Company", "we", "our", "us"). By utilizing our web hosting infrastructure, services, and website (altius.host), you ("Client", "User") agree to comply with and be bound by the following Terms of Service and Acceptable Use Policy.

Important: By agreeing to these Terms of Service, you also acknowledge and agree to our Privacy Policy, our Refund Policy, and — where you use our infrastructure to process personal data that is subject to a data protection law imposing obligations on controllers and processors — our Data Processing Agreement, which forms an integral part of these Terms.

Where you order a service governed by a Service Schedule appended to these Terms — Schedule A (Managed Edge Security) or Schedule B (Professional Services) — that Schedule also applies to you and forms part of these Terms. Schedule C (Switching and Data Portability) applies to Clients established in the European Union or the European Economic Area. In the event of a conflict concerning that service, the Schedule prevails.

2. Eligibility and Capacity

To open an account you must be at least eighteen (18) years of age and legally capable of entering into a binding contract. Where you register on behalf of a company or other legal entity, you represent that you are authorised to bind that entity, and "Client" refers to that entity.

We may decline to open, or may close, any account where these conditions are not met.

3. Company Information, Jurisdiction and Governing Law

ALTIUS HOST LLC is a registered entity in the State of New Mexico, USA (Address: 8206 Louisiana Blvd NE, Ste A #9372, Albuquerque, NM 87113). These Terms shall be governed by and construed in accordance with the laws of the State of New Mexico, without regard to its conflict of law provisions. We operate globally, providing enterprise-grade web hosting solutions. Our physical server infrastructure is securely housed in premium, highly compliant data centres located within the European Union. Servers are currently operated in Germany and Finland; additional European locations may be brought into service over time, and all are and will remain within the European Economic Area. The current list is maintained in our Data Processing Agreement.

Nothing in these Terms limits any mandatory statutory rights available to consumers under the law of their country of residence, nor deprives a consumer of the protection of the mandatory provisions of the law of the country in which they are habitually resident.

4. Provision of Services and Client Responsibilities

ALTIUS HOST LLC strives to provide uninterrupted network and server access. However, we cannot guarantee that the service will be entirely error-free or uninterrupted due to the nature of complex digital infrastructure.

- **Service Level Agreement (SLA):** We guarantee a 99.9% network and server uptime for our hosting services. In the event this SLA is not met in a given calendar month, eligible clients may request a prorated credit to their hosting account. SLA credit requests must be submitted through the client portal within thirty (30) days of the end of the affected calendar month, and must reference the approximate dates and times of the unavailability. We will respond to credit requests within ten (10) business days. Credits are applied to the Client's account balance and are not redeemable for cash. This SLA does not apply to scheduled

maintenance, third-party network outages, Client-caused outages (including application errors, resource exhaustion, or misconfiguration), or circumstances beyond our reasonable control.

- **Scheduled Maintenance:** We will give at least forty-eight (48) hours' notice of planned maintenance expected to cause service interruption, except where emergency security patching requires immediate action.
- **Data Backups:** We perform an automated backup of hosted accounts **once daily**. Backups are incremental, are transferred over an encrypted connection, and are stored, unencrypted, on separate backup storage within the European Economic Area. We keep the **seven (7) most recent daily backups** on a rolling basis: each backup is retained for up to seven days before being removed by a later cycle. The backup storage also keeps daily snapshots of itself for seven (7) days to protect the backup system; a removed backup may therefore remain in those snapshots for up to seven further days, but snapshots are not offered as additional restore points. The Client can restore files, databases, and email from the available backups through the backup tool in the control panel. We do not retain point-in-time or long-term archival backups beyond these periods. Backups of a terminated account are retained as described in Section 7.
- **No Warranty as to Backups:** Backups are provided on a **best-effort, as-is basis and without warranty of any kind**. We do not guarantee that any backup archive will exist, be complete, be free of corruption, be restorable, or be available at any particular time. Our backup storage resides on leased third-party cloud and hardware infrastructure over which we exercise no direct physical control, and failures, corruption, latency, or loss originating within that infrastructure are outside our control. We accept no liability for the unavailability, incompleteness, corruption, or failed restoration of any backup.
- **Client Backup Responsibility:** The Client is **solely and ultimately responsible** for maintaining independent, off-platform backups of all website content, databases, email, and configuration files. Where data loss or corruption is not identified within the seven-day rotation window, the affected data will not be recoverable from our systems. Our backups are an operational convenience only and must not be relied upon as the Client's backup strategy, as an archival record, or as a disaster recovery solution.
- **Migration Assistance:** Where a plan includes free migration, our engineers transfer the existing websites or hosting accounts covered by the plan specification, up to the number stated there, to the new account on a reasonable-efforts basis, once the Client has provided the access required. The Client remains responsible for keeping its own complete copy of the data until the migration has been confirmed, and for any changes required at the previous provider or registrar.
- **Account Security:** The Client is responsible for maintaining the confidentiality of their login credentials and for any activities that occur under their account. The Client must notify us without delay of any suspected unauthorised access.
- **Automation, API Access and AI Agents:** The Client may connect our services to automation tools, AI agents, and other third-party software, including through the Model Context Protocol (MCP) interface available in the cPanel control panel and in the Elementor WordPress page builder. Any action performed through such a connection — including an action executed by an AI agent without the Client's contemporaneous review — is treated as an action performed by the Client, is subject to these Terms and the Acceptable Use Policy, and is the Client's sole responsibility. We do not review, approve, or warrant the outcome of automated or AI-generated changes. We strongly recommend that the Client maintains current independent backups before authorising any agent to modify a hosted account or website.
- **Integration Credentials:** API tokens, application passwords, MCP connection files, and similar credentials issued to or created by the Client are account credentials within the meaning of the Account Security provision above. The Client must store them securely, limit them to the minimum permissions required, and revoke them without delay when they are no longer needed or are suspected to be compromised.
- **Third-Party AI Services:** AI models and agents that the Client connects to its account are provided by third parties selected by the Client, including the provider of the Client's AI assistant and WebPros, the owner of cPanel, whose MCP connection the Client activates using its own WebPros account. When selected and connected by the Client, these providers are not our sub-processors, and any personal data the Client transmits to them is transmitted by the Client as controller and under that provider's own terms. Providers

that we ourselves use to operate and support the services are engaged as our sub-processors and are listed in our Data Processing Agreement.

- **Lawful Content:** The Client is solely responsible for the legality of all content stored, transmitted, or published using our infrastructure, and for obtaining any licences, consents, or registrations required for that content.

5. Billing, Payments, and Taxes

All services are billed exclusively through our automated billing portal. Payments are securely processed through a certified US-based payment processor, and funds are held in a US financial institution.

- **Currency:** All services are quoted and charged in **United States Dollars (USD)**. Where your payment instrument is denominated in another currency, your card issuer or bank applies its own conversion rate and any associated fees, over which we have no control.
- **Taxes:** Prices are quoted exclusive of tax. Where we are required by law to charge Value Added Tax (VAT), Goods and Services Tax (GST), or a comparable consumption tax on a supply to you, that tax is added at checkout at the rate applicable in your country and is shown as a separate line on the invoice. At present, VAT is charged only to clients located in European Union member states or in the United Kingdom. For clients located elsewhere, no tax is currently added, and the quoted price is the price payable unless the tax treatment shown at checkout states otherwise.
- **Business clients and reverse charge:** Where an EU business client supplies a valid VAT identification number that we are able to validate, the reverse charge mechanism is applied automatically and no VAT is charged by us; responsibility for accounting for the tax passes to the client. The Client is responsible for the accuracy of any VAT identification number supplied and for any liability arising from an invalid, expired, or incorrectly entered number.
- **Changes in tax obligations:** Our tax registrations, and the countries in which we are required to charge tax, may change over time as our operations develop. Any such change takes effect prospectively and is applied automatically at checkout and on invoices. The tax treatment applicable to your country is always shown before you confirm an order, and the invoice you receive sets out the final amount payable.
- **Renewals:** Services are automatically invoiced prior to the end of the current billing cycle to prevent service interruption.
- **Renewal Pricing:** Introductory, promotional, and first-term prices apply only to the initial billing period unless expressly stated otherwise. Renewals are charged at our standard rate in effect at the time of renewal. We will give at least thirty (30) days' notice by email before any increase to a recurring price takes effect, and the Client may cancel before the renewal date to avoid the new rate.
- **Immediate Performance (EEA and UK Consumers):** Because our services are supplied digitally and activated upon payment — immediately for most services, and within one business day for Managed Node plans — consumers resident in an EEA member state or the United Kingdom are asked at checkout to expressly request immediate commencement of the service and to acknowledge that doing so affects the statutory right of withdrawal as described in our Refund Policy.

6. Invoicing, Overdue Payments and Suspension

- **Invoice Generation:** Renewal invoices are generated automatically **fourteen (14) days** before the due date.
- **Reminders:** A payment reminder is sent seven (7) days before the due date. Where an invoice remains unpaid, overdue notices are sent one (1), three (3), and seven (7) days after the due date.
- **Suspension:** Where payment has not been received **seven (7) days** after the due date, the service is suspended. Content remains stored but is not publicly accessible, and a suspension notice is sent to the Client.
- **Automatic Unsuspension:** Services are reactivated automatically upon receipt of payment, and the Client is notified.

- **Invoice Cancellation:** Unpaid invoices are automatically cancelled **fourteen (14) days** after the due date. Cancellation of an invoice does not cancel the underlying service or extinguish the Client's obligation to pay for services already rendered.
- **Termination and Deletion:** Where payment has not been received **thirty (30) days** after the due date, the account is terminated and its websites, databases, and email are deleted from our servers. Backups of the terminated account are retained for thirty (30) days, as described in Section 7, and are then permanently deleted. Deleted data cannot be recovered.

No late payment fee is applied. It is the Client's responsibility to keep a valid billing email address and payment method on file.

7. Cancellation, Termination by the Client, and Data Retention

- **Cancellation:** The Client may cancel any service at any time through the client portal. Because renewal invoices are generated fourteen (14) days in advance, cancellation requests should be submitted at least **fifteen (15) calendar days** before the renewal date to prevent a renewal invoice being raised. Cancellations may be set to take effect immediately or at the end of the current paid period; accounts with a cancellation request are terminated automatically on the requested date.
- **Effect of Cancellation:** Unless a refund applies under the Refund Policy, cancellation does not entitle the Client to a refund of fees already paid for the current billing period. Service remains available until the end of the paid period where end-of-period cancellation is selected.
- **Data Export:** The Client is responsible for exporting all website content, databases, and email data before the cancellation takes effect. Export tools are available through the client portal at all times while the account is active.
- **Post-Termination Retention:** Following termination — on the cancellation date or for non-payment — the account and its data are deleted from our servers, and the account's backups are retained for **thirty (30) days**, during which the Client may request that the account be restored from them. After this period, the backups are permanently and automatically deleted, and any residual copies in the daily snapshots of our backup storage are removed within a further seven (7) days. Data deleted following termination cannot be recovered. The retrieval of data after a switching request is governed by Schedule C.
- **Accounts Terminated for AUP Violations:** Where an account is terminated for a violation of the Acceptable Use Policy, we reserve the right to delete data immediately and without a retention period, particularly where continued storage would itself be unlawful.

8. Infrastructure and Acceptable Use Policy (AUP)

Our sovereign digital infrastructure is optimized for high-performance CloudLinux Isolated Environments. To maintain the highest level of performance, security, and stability, we strictly enforce a zero-tolerance policy against the following activities:

- **Resource Abuse:** Our stack (including LiteSpeed, Redis, and QUIC.cloud) is optimized for web hosting workloads. Across all plan tiers — WP Hosting, Business Hosting, and Managed Infrastructure — using accounts for mass file storage, backup dumping, video streaming portals, or deploying scripts that unnaturally exhaust CPU, RAM, or I/O resources is prohibited.
- **Spam and Mass Emailing:** The transmission of unsolicited commercial email (UCE) or unsolicited bulk email (UBE) is strictly prohibited. This includes maintaining open SMTP relays or hosting sites advertised via spam.
- **Malware, Phishing, and Hacking:** Hosting, distributing, or linking to malicious software, phishing pages, botnets, or engaging in unauthorized system access (hacking) is strictly forbidden.
- **Cryptocurrency Mining:** Any deployment of scripts, daemons, or software intended to mine cryptocurrency is prohibited.

- **Illegal and Adult Content:** We do not permit the hosting of adult content, pornography, or material that violates local, state, national, or international laws — including the national law of whichever country your account is hosted in and European Union law. This includes copyright infringement and piracy.
- **Network Abuse:** Port scanning, denial-of-service activity, traffic amplification, and any attempt to circumvent resource limits or account isolation are prohibited.
- **Automated and AI-Driven Activity:** The prohibitions in this section apply equally to activity carried out by scripts, automation tools, or AI agents operating through the Client's account, including request volumes to control panel, API, or MCP interfaces that degrade shared infrastructure.

Reporting abuse. Suspected violations of this AUP originating from our network may be reported to **abuse@altius.host**. We investigate all credible reports and respond in accordance with the severity of the issue.

9. Copyright Infringement and DMCA Notices

ALTIUS HOST LLC respects the intellectual property rights of others and responds to notices of alleged copyright infringement in accordance with the Digital Millennium Copyright Act (17 U.S.C. § 512).

Notices of claimed infringement should be submitted to our designated agent as set out on our DMCA Policy page. We reserve the right to remove or disable access to allegedly infringing material and to terminate the accounts of repeat infringers.

10. Reporting Illegal Content

We do not permit our infrastructure to be used to host content that is unlawful under any law applicable to us, to the Client, or to the jurisdiction in which our servers are located. The mechanisms set out in this section are available to anyone, anywhere, and we operate them as a matter of standing policy for all clients irrespective of location.

Where and to the extent that these services fall within the scope of Regulation (EU) 2022/2065 (the Digital Services Act) or any comparable notice-and-action regime, the provisions below are intended to satisfy the corresponding requirements.

- **Notice and action mechanism:** Any individual or entity may notify us of content hosted on our infrastructure that they consider to be illegal, by submitting a notice to **abuse@altius.host**. To allow us to act, a notice should contain: a sufficiently substantiated explanation of why the content is considered illegal; the exact URL or URLs at which the content is located; the name and email address of the notifying party (except where the notice concerns suspected child sexual abuse material or other offences where anonymity is appropriate); and a statement confirming the notifying party's good faith belief that the information in the notice is accurate and complete. We will send confirmation of receipt without undue delay and will process notices in a timely, diligent, non-arbitrary, and objective manner. Once a decision has been taken, we will inform the notifying party of that decision without undue delay, together with the available possibilities for redress.
- **Point of contact for authorities:** Courts, regulators, and other competent public authorities may contact us electronically at **legal@altius.host**. Communication may be conducted in **English**.
- **Point of contact for recipients:** Recipients of our services may contact us electronically at **support@altius.host** or through the client portal, in **English**.
- **Statement of reasons:** Where we restrict, remove, disable, suspend, or terminate access to content or to an account on the ground that the content is illegal or incompatible with our Acceptable Use Policy, we will provide the affected Client with a clear and specific statement of reasons. That statement will identify the restriction imposed and its territorial scope, the facts and circumstances relied upon, whether automated means were used, the legal or contractual ground relied upon, and the avenues available to the Client to contest the decision.

- **Contesting a decision:** A Client who considers a restriction to be unfounded may respond to the statement of reasons through the client portal. We will review such responses promptly and without reliance on automated means alone.

11. Third-Party Software and Licences

Our services include third-party software licensed to us or to the Client, including **cPanel and WHM** (control panel), **CloudLinux** (account isolation and resource management), **LiteSpeed Web Server**, **Redis**, **QUIC.cloud**, **Imunify360** (malware scanning and application-layer security), **ModSecurity** (server-side web application firewall rules), **ConfigServer Security & Firewall** (perimeter firewalling and intrusion detection), and **JetBackup** (account backups). Where the Client orders Managed Edge Security, that service is delivered through **Cloudflare** (DNS, content delivery, web application firewalling, and DDoS mitigation) within the Client's own Cloudflare account, as described in Schedule A. Use of such software is subject to the licence terms of the respective vendor, which are incorporated by reference where applicable.

Our hosting plans also provide access to the cPanel Meridian interface and its Model Context Protocol (MCP) connection, which is supplied by WebPros and becomes available once the Client links its own WebPros account. The Meridian interface also includes an AI Assistant, supplied by WebPros and enabled by us on our hosting plans. The AI Assistant answers questions about the Client's own hosting account and, where the Client approves a proposed change, can carry out routine account tasks such as creating an email account. It operates only within the Client's own account, is subject to the usage limits set by WebPros, and does not replace our support. Changes the Client approves through the AI Assistant are the Client's own actions for the purposes of Section 4. WebPros processes AI Assistant conversations as our sub-processor, as set out in our Data Processing Agreement. Where the Client uses the Elementor WordPress page builder, including its MCP feature, Elementor is licensed to the Client directly by its vendor. Licences for Elementor Pro or any other premium plugin are not included in any hosting plan unless expressly stated in the plan specification.

Where a licence is provided as part of a hosting plan, it remains valid only for the duration of the associated service and terminates automatically upon cancellation or termination. The Client may not resell, redistribute, or transfer any such licence independently of the service.

We do not warrant any third-party software and are not liable for defects, vulnerabilities, or discontinuation of products supplied by third parties, save to the extent of our own negligence.

12. Domain Name Registrations

Domain names are registered, transferred, and renewed through our registrar partner **Namecheap**. Such registrations are additionally subject to the policies of the relevant registry, registrar, and ICANN, including applicable dispute resolution policies.

- **Registrant responsibilities:** The Client is the registrant and is responsible for supplying and maintaining **accurate and current** registration contact data. Inaccurate or unverified data may result in suspension or cancellation of the domain by the registrar or registry.
- **Renewal:** Renewal of a domain is the Client's responsibility. Renewal reminders are sent thirty (30) and seven (7) days before the expiry date, and again three (3) days after expiry.
- **Grace Period:** Following expiry, a **twenty-five (25) day** grace period applies, during which the domain may be renewed at the standard renewal price with no additional fee.
- **Redemption Period:** After the grace period, a **thirty (30) day** redemption period applies. Restoration during this period is subject to a redemption fee of **USD 100.00** in addition to the renewal price. This fee is set by the registry and is not refundable.
- **Expiry:** After the redemption period, the domain is released and may be registered by any third party. We cannot guarantee recovery of a released domain.

- **Included add-ons:** DNS management, email forwarding, and ID Protection (WHOIS privacy, where the registry permits it) are provided at no charge.
- **Managed Edge Security:** Where a domain registered through us is enrolled in Managed Edge Security, we set its nameservers, on the Client's instruction, to those assigned by Cloudflare to the Client's own Cloudflare account, and configure its DNS and security settings through the access the Client grants us, as described in Schedule A. Enrolment does not change registrant status: the Client remains the registrant of the domain.
- Domain registrations are separate from hosting services and are not refundable (see Refund Policy).

13. Export Control and Sanctions Compliance

As a United States entity, ALTIUS HOST LLC is subject to United States export control and economic sanctions laws. The Client represents and warrants that it is not located in, organised under the laws of, or ordinarily resident in a jurisdiction subject to comprehensive United States sanctions, and that it is not listed on any applicable restricted-party list maintained by the United States, the European Union, or the United Nations.

The Client further undertakes not to use the services for any purpose prohibited by applicable export control or sanctions law. We may suspend or terminate any account immediately where we reasonably believe this section has been or may be breached.

14. Account Suspension and Termination by the Company

ALTIUS HOST LLC reserves the right to suspend or terminate any account immediately, without prior notice, if a violation of this AUP is detected. Where circumstances reasonably permit, we will notify the Client and provide an opportunity to remedy the violation. We reserve the right to refuse service to anyone at our sole discretion.

15. Limitation of Liability and Indemnification

In no event shall ALTIUS HOST LLC, its directors, employees, or partners be liable for any indirect, incidental, special, consequential, or punitive damages, including without limitation, loss of profits, data, use, goodwill, or other intangible losses, resulting from your access to or use of or inability to access or use the Service.

To the maximum extent permitted by applicable law, our total aggregate liability arising out of or relating to the services in any twelve (12) month period shall not exceed the total amount paid by the Client to ALTIUS HOST LLC for the affected service during that period.

We deliver our services using leased third-party data centre, network, and cloud storage infrastructure. We are not liable for loss, corruption, interruption, or degradation originating within that infrastructure or within any third-party provider's systems, including failures of storage hardware, hypervisors, network fabric, or upstream connectivity, save to the extent such loss results from our own negligence.

The Client agrees to indemnify and hold harmless ALTIUS HOST LLC against claims brought by third parties, and against related losses and reasonable costs, to the extent arising from the Client's content, from the Client's breach of these Terms or of the Acceptable Use Policy, or from the Client's violation of applicable law. This indemnity does not apply to a consumer to the extent that it would be inconsistent with mandatory consumer protection law.

Nothing in this section excludes or limits liability for death or personal injury caused by negligence, for fraud or fraudulent misrepresentation, or for any other liability that cannot lawfully be excluded — including, for consumers, liability under mandatory consumer protection law.

16. Force Majeure

Neither party shall be liable for any failure or delay in performance caused by circumstances beyond its reasonable control, including natural disasters, war, terrorism, civil unrest, epidemic, labour disputes, failures of upstream network providers, sustained denial-of-service attacks, power or data centre failures, changes in law,

or acts of government. The affected party will notify the other without undue delay and use reasonable efforts to resume performance.

Where such circumstances persist for more than thirty (30) consecutive days, either party may terminate the affected service, and the Client is entitled to a pro-rata refund of prepaid fees covering the unused period.

17. Changes to These Terms

We may update these Terms of Service, the Acceptable Use Policy, and any linked policies from time to time to reflect changes in our services, our infrastructure, or applicable law.

- **Notice:** Material changes will be announced at least thirty (30) days in advance by email to the address registered on the Client's account and by notice within the client portal. Non-material changes (clarifications, corrections, contact detail updates) take effect upon publication.
- **Acceptance:** Continued use of the services after the effective date of a change constitutes acceptance of the revised Terms.
- **Right to Reject:** A Client who does not accept a material change may cancel the affected services before the effective date and receive a pro-rata refund of any prepaid fees covering the unused remainder of the current billing period.
- **Version History:** The "Last Updated" date at the top of this document reflects the most recent revision.

18. General Provisions

- **Entire Agreement:** These Terms, together with any applicable Service Schedule, the Privacy Policy, Refund Policy, Data Processing Agreement, and any order form or plan specification, constitute the entire agreement between the parties and supersede all prior representations and understandings relating to the services.
- **Severability:** If any provision is held to be invalid or unenforceable, that provision shall be modified to the minimum extent necessary, or severed, and the remaining provisions shall remain in full force.
- **No Waiver:** A failure or delay in exercising any right under these Terms does not constitute a waiver of that right.
- **Assignment:** The Client may not assign or transfer its rights or obligations without our prior written consent. We may assign these Terms in connection with a merger, acquisition, or sale of assets, on notice to the Client.
- **No Third-Party Beneficiaries:** These Terms do not confer any rights on any person other than the parties.
- **Notices:** Notices to the Client are given by email to the address registered on the account, or by notice within the client portal. Notices to us should be sent through the client portal or to the contact addresses below.
- **Language:** These Terms are drafted in English. Any translation is provided for convenience only; the English version governs.
- **Survival:** Sections relating to billing, limitation of liability, indemnification, export control, and general provisions survive termination.

19. Contact

ALTIUS HOST LLC

8206 Louisiana Blvd NE, Ste A #9372

Albuquerque, NM 87113, United States

General enquiries: contact form

Privacy and data protection: privacy@altius.host

Copyright notices: dmca@altius.host

Illegal content notices and abuse reports: abuse@altius.host

Point of contact for courts, regulators and public authorities: legal@altius.host

Point of contact for clients and service recipients: support@altius.host

Billing enquiries: billing@altius.host

Schedule A — Managed Edge Security

A.1 Scope and Eligibility. Managed Edge Security is available only for domains that are registered through ALTIUS HOST LLC and whose website is hosted on our infrastructure. Server-side security services performed on our own infrastructure, such as Account Hardening, are provided under Section 4 of these Terms and are not part of Managed Edge Security. The service consists of the configuration, maintenance, and monitoring of the domain's DNS, TLS, web application firewall, bot and vulnerability-scanner mitigation, and related security settings within the Client's own Cloudflare account. The Cloudflare features available depend on the Cloudflare plan to which the Client subscribes.

A.2 The Client's Cloudflare Account. The Client holds its Cloudflare account in its own name, accepts Cloudflare's terms directly, and pays Cloudflare directly for any paid Cloudflare plan it chooses. Cloudflare provides its services to the Client, not to us. The Client retains the Super Administrator role and full control of the account at all times.

A.3 Access and Authorisation. To receive the service, the Client invites the user account designated by us as a member of the Client's Cloudflare account with the Administrator role, which does not permit changes to billing or account membership. The Client gives the authorisation set out below by ordering the service, by confirming it on the order form where the service is included in a hosting plan, or by requesting activation through the client portal at any later time; the authorisation has the same form and effect however it is given. By giving that authorisation and granting this access, the Client expressly authorises us, for the duration of the service, to: (a) change the domain's nameservers at the registrar to those assigned by Cloudflare to the Client's account; (b) create, modify, and delete DNS records for the domain; and (c) configure and maintain the domain's security, performance, and TLS settings. Where a hosting plan includes Managed Edge Security but the Client has not yet given the authorisation and granted access, that component of the plan remains inactive until the Client does so; the remainder of the plan is unaffected and no separate charge arises. The Client may withdraw this authorisation at any time by revoking our membership, whereupon the service ends and Section A.9 applies. We protect our member account with multi-factor authentication and use it only to perform the service.

A.4 DNS Records and Email. At onboarding, we review the domain's existing DNS records and ask the Client to confirm the zone before the nameservers are changed. The Client is responsible for the completeness and accuracy of the records it supplies or confirms, including mail (MX), SPF, DKIM, DMARC, and third-party verification records. Omitted or incorrect records may interrupt email delivery or third-party services. Changes to DNS records are requested through the client portal by the Client or its authorised contacts; we aim to implement routine changes within one (1) business day. We may make changes without prior request where urgently required to protect the domain or our infrastructure, and will notify the Client promptly. Changes made directly by the Client or by third parties in the Client's Cloudflare account are the Client's responsibility.

A.5 Security Decisions and False Positives. Security rules may block, challenge, or rate-limit requests, and may occasionally affect legitimate visitors, integrations, or automated services. We will review and adjust rules on the Client's request, including allowlisting specific services where this can be done safely. To the extent permitted by law, we are not liable for loss of traffic, revenue, or business resulting from security measures applied in good faith.

A.6 No Guarantee. Managed Edge Security is provided on a reasonable-efforts basis. No security service can prevent every attack, and this service does not replace secure application development, timely software updates, strong credentials, or independent backups, which remain the Client's responsibility. The availability of the Cloudflare network is a third-party service within the meaning of the SLA exclusions in Section 4, and Cloudflare's own decisions concerning the Client's account are outside our control.

A.7 Security Data. Through our access, we may review request metadata and security-event records relating to visitors of the Client's website solely to configure, monitor, and report on the service. This processing is carried out on the Client's behalf under our Data Processing Agreement.

A.8 DNSSEC. DNSSEC may be enabled for enrolled domains. Before any change of nameservers, DNSSEC must be disabled and the corresponding DS record removed from the registry, or the domain may become unreachable. We coordinate this step with the Client.

A.9 Cancellation and Exit. On cancellation or termination of Managed Edge Security, we cease all changes to the Client's Cloudflare account, remove our member access or ask the Client to revoke it, and provide the Client with a summary of the configuration applied. The domain, its DNS zone, and its configuration remain in the Client's own Cloudflare account. If the Client wishes to move the domain away from Cloudflare, the Client is responsible for preparing the new DNS provider; where the domain is still registered through us, we change the nameservers on the Client's instruction after DNSSEC has been disabled as described in Section A.8.

A.10 Relationship to Hosting. If the hosting service for the domain is terminated, Managed Edge Security for that domain ends at the same time and Section A.9 applies.

A.11 Fees and Refunds. Where Managed Edge Security is purchased as a standalone service, it is billed per domain as a recurring service and is not covered by the 30-day money-back guarantee (Refund Policy, Section 2).

Where Managed Edge Security is included in a hosting plan at no separate charge, the billing and refund terms of that plan apply to it instead: it is not billed per domain, and the exclusion from the 30-day money-back guarantee does not apply to it. The number of domains covered is that stated in the plan specification; enrolment of additional domains is charged as a standalone service under the preceding paragraph.

In either case, our fees cover configuration, maintenance, and monitoring only; any Cloudflare subscription is paid by the Client directly to Cloudflare.

A.12 Changes to Provider Features. Where Cloudflare withdraws or materially changes a feature on which the service relies, we will substitute a reasonably equivalent measure or notify the Client, who may then cancel the affected service and receive a pro-rata refund of prepaid fees for the unused period.

Schedule B — Professional Services

B.1 Scope. This Schedule applies to website maintenance, search engine optimisation, digital marketing, brand identity, and other professional services ("Professional Services"). The scope, deliverables, number of included revisions, and timelines are those set out in the plan specification or in a written order or statement of work agreed with the Client.

B.2 Client Cooperation. The Client will provide timely access, content, materials, and approvals. Timelines are extended by any period of delay in the Client's cooperation.

B.3 Revisions and Acceptance. Each deliverable includes the number of revision rounds stated in the order. A deliverable is deemed accepted ten (10) business days after delivery unless the Client notifies us in writing of a material non-conformity with the agreed scope.

B.4 No Guaranteed Results. Search engine rankings, traffic, conversions, and revenue depend on factors outside our control, including search engine algorithms, advertising platform policies, competition, and market conditions. We do not guarantee any particular ranking, position, traffic level, or commercial result.

B.5 Third-Party Platforms and Advertising Spend. Advertising budgets are paid by the Client directly to the relevant platform and are not included in our fees. The Client's accounts on third-party platforms are subject to those platforms' terms, and we are not responsible for suspensions, policy decisions, or changes made by them.

B.6 Intellectual Property. Upon full payment, the Client owns the final deliverables created specifically for it. We retain ownership of our pre-existing materials, tools, templates, and know-how, and grant the Client a perpetual licence to use any of them incorporated in the deliverables. Third-party assets such as fonts, stock imagery, or plugins remain subject to their own licences. We will not display the Client's work in our portfolio without the Client's prior written consent.

B.7 Access Credentials. Credentials provided to us are used only to perform the Professional Services, are limited to the permissions required, and should be revoked or changed by the Client when the engagement ends.

B.8 Maintenance Services. Software updates may introduce incompatibilities with themes, plugins, or custom code. We take a backup before scheduled updates and, where an update causes a problem, restore the website to its pre-update state where possible. We are not responsible for defects in third-party software.

B.9 Term and Cancellation. Recurring Professional Services may be cancelled with thirty (30) days' notice, effective at the end of the billing period in which the notice period ends. Fees for one-time or bespoke work are non-refundable once work has commenced (Refund Policy, Section 2). Larger projects may be invoiced in milestones as set out in the order.

B.10 Confidentiality. We treat all non-public information received from the Client in connection with the Professional Services as confidential and use it only to perform those services.

Schedule C — Switching and Data Portability (EU Data Act)

C.1 Scope. This Schedule implements Chapter VI of Regulation (EU) 2023/2854 (the Data Act) and applies to Clients established in the European Union or the European Economic Area who receive hosting or cloud services from us. Where this Schedule conflicts with any other provision of these Terms, this Schedule prevails for those Clients. Nothing in this Schedule limits rights available to any Client under Section 7.

C.2 Right to Switch. The Client has the right to switch to another provider of an equivalent service, to port its exportable data and digital assets to its own on-premises infrastructure, or to use more than one provider in parallel. We will not impose, and will remove, any commercial, technical, contractual, or organisational obstacle to the exercise of that right.

C.3 Notice. The Client may begin the switching process at any time by giving notice through the client portal. The maximum notice period we require is **two (2) months**; the Client may specify a shorter period, and we will act on it where we reasonably can.

C.4 Transitional Period. On expiry of the notice period, a **transitional period of thirty (30) calendar days** begins, during which we continue to provide the service, maintain business continuity, and maintain the same level of security. The Client may request a longer transitional period more appropriate to its own purposes. Where completing the switch within thirty (30) days is technically unfeasible, we will notify the Client within **fourteen (14) working days** of the switching request, explain the technical reasons in writing, and set an extended period, which will not exceed **seven (7) months**.

C.5 Assistance. During the notice and transitional periods we will exercise due care to maintain continuity, act in good faith, provide the Client with the information and technical support it reasonably needs, and cooperate in good faith with the destination provider, including by making available the documentation and interfaces required to complete the transfer.

C.6 Exportable Data and Digital Assets. The following are exportable and will be made available in a structured, commonly used, and machine-readable open format:

- website files and directory structure, as standard archives;
- databases, as standard SQL dumps;
- email mailboxes and messages, in standard mailbox formats, together with mail routing configuration;
- DNS zone records, as standard zone files;
- TLS certificates and private keys held in the account;
- application, server, and account configuration data exposed through the control panel;
- account metadata that the Client has provided or generated.

An up-to-date register of these data structures, formats, standards, and open interoperability specifications is maintained at altius.host/switching and referenced in Section C.11.

C.7 Excluded Data. Data specific to the internal functioning of our infrastructure — including our own monitoring and orchestration records, security event logs relating to our platform as a whole, and any material whose disclosure would compromise the security of our infrastructure or the trade secrets of a third party — is not exportable. We will identify any such exclusion to the Client on request.

C.8 Data Retrieval Period and Erasure. After the transitional period ends, the Client has a **retrieval period of at least thirty (30) calendar days** in which to retrieve its exportable data and digital assets. On expiry of that period, or at the Client's earlier written request, we erase all exportable data and digital assets and confirm the erasure to the Client in writing. Backups of the account are deleted together with that data, and any residual copies in the daily snapshots of our backup storage are removed within a further seven (7) days.

C.9 Switching Charges. We do not charge for the exercise of switching rights — including data export and assistance during a switch — and we do not apply any early termination penalty in connection with switching. Standard service fees for the period during which the service continues to be provided remain payable.

C.10 Functional Equivalence and Interoperability. Where we provide infrastructure-level services, we take all reasonable measures to enable the Client to achieve functional equivalence after the switch. For all other services we make open interfaces available free of charge and export data in a structured, commonly used, machine-readable format, using open interoperability specifications where these exist for the service concerned.

C.11 Information Published on Our Website. Before contracting, and at all times thereafter, we publish at **altius.host/switching**: the available switching and porting procedures, methods, and formats; any known technical restrictions or limitations; the register of data structures and formats described in Section C.6; and details of any standard service fees, switching charges, and early termination penalties.

C.12 Jurisdiction and Governmental Access. Our hosting infrastructure is located within the European Economic Area. Our corporate entity is established in the United States, and our client portal, billing, and support platform is hosted in the United States, as set out in our Data Processing Agreement. We apply reasonable technical, organisational, and legal measures to prevent international or third-country governmental access to non-personal data held in the European Union where such access would conflict with Union or Member State law, including assessment of the legal basis of any request received, challenge of requests that appear unlawful or disproportionate, and disclosure of the minimum data necessary where disclosure is legally compelled. Where the law permits, we notify the affected Client before disclosing any data.

C.13 Termination on Completion. Where the Client has given notice to switch, the contract for the affected services terminates upon successful completion of the switching process, and we notify the Client of the termination. Where the Client has given notice that it wishes only to have its exportable data and digital assets erased, without switching, the contract terminates at the end of the notice period.

For your administrative records, you may download an official copy of the ALTIUS HOST LLC Terms of Service & Acceptable Use Policy.