Pladinum Group SL
Avenida Manolete 3a
29660 Marbella, Málaga (ES)
+34 697 9898 40

www.pladinum.com
billing@pladinum.com

CIF: ES B72758436
IBAN: ES1400497363182210017915
BIC: BSCHESMM

Acceptable Use Policy

Last revised: 17 June 2026

1. Purpose and Scope

1.1 This Acceptable Use Policy ("AUP") sets out the rules governing the use of the products, services, and solutions made available by Pladinum Group SL ("Pladinum", "we", "us", "our"). It forms an integral part of the Agreement between Pladinum and the Customer and is incorporated by reference into the General Terms and Conditions.

1.2 Applicable Services. This AUP applies to all Pladinum Services, including shared hosting, managed WordPress hosting, WooCommerce hosting, VPS hosting, dedicated server hosting, reseller hosting, email hosting, ecommerce hosting, business email, domain name services, SSL certificates, backup and disaster recovery, website protection, VPN, and server administration. It does not apply to Cryptvice hardware products, which are governed by their own separate terms.

1.3 Responsibility for Users. You are responsible for your own use of the Services and for the activities of all persons who access the Services through your account, including your employees, agents, customers, and end users ("Users"). You must ensure that all Users comply with this AUP, and any breach by a User is treated as a breach by you.

1.4 Acceptance. By accessing or using the Services, you agree to be bound by this AUP. If you do not agree with it, you must not access or use the Services.

1.5 Determination. Whether any content or activity violates this AUP is determined by Pladinum acting reasonably. The examples given in this AUP are illustrative and not exhaustive.

2. General Principles

2.1 Lawful use. The Services must be used only for lawful purposes and in compliance with all applicable laws and regulations, including the laws of Spain and of the European Union, and the laws of any jurisdiction from which you operate or to which your content is directed.

2.2 No harm. You must not use the Services in any way that is illegal or fraudulent, that infringes the rights of others, that harms or threatens the security, integrity, or availability of the Services, our infrastructure, or other customers, or that exposes Pladinum to legal liability or reputational harm.

2.3 Legitimate purpose. The Services are provided for the purposes described on our website and in your plan. You must not use the Services for any activity for which they are not intended or promoted.

3. Prohibited Content

3.1 You must not use the Services to host, store, transmit, publish, or link to any content that: (i) is illegal under any applicable law; (ii) infringes or misappropriates any intellectual property right, including copyright, trademark, patent, or trade secret, or any privacy, publicity, or other personal right; (iii) is defamatory, false, misleading, deceptive, or fraudulent; (iv) is obscene, or that sexually exploits or endangers minors; or (v) promotes terrorism, violence, discrimination, racism, hatred, harassment, human trafficking, or harm against any individual or group.

3.2 Personal data. You must not publish or distribute the personal data of others without a lawful basis and the consents required under applicable data protection law.

3.3 Adult content. Lawful adult content is permitted only on VPS and dedicated server plans. It is not permitted on shared hosting, reseller hosting, or managed WordPress plans. Where permitted, such content must comply with all applicable laws, including age-verification and record-keeping requirements. Content that is illegal under any applicable law — and child sexual abuse material in particular — is never permitted on any plan (see Section 9).

4. Prohibited Activities

4.1 Network and security abuse. You must not attempt to gain unauthorised access to, scan, probe, or test the vulnerability of any system, network, or account that you are not authorised to access; interfere with or disrupt any user, host, or network (including through denial-of-service or distributed denial-of-service attacks, flooding, or deliberate attempts to overload a system); or evade, disable, or circumvent any security or authentication measure.

4.2 Malicious code. You must not host, distribute, or transmit viruses, worms, trojans, ransomware, exploit kits, botnet command-and-control infrastructure, or any other malicious code.

4.3 Fraud and deception. You must not use the Services for phishing, spoofing, identity theft, carding, advance-fee ("419") fraud, pyramid or Ponzi schemes, chain letters, or any other fraudulent or deceptive activity.

4.4 Spam. You must not send unsolicited bulk or commercial communications, operate or support open mail relays or open proxies, or use the Services to host or promote material that is advertised through spam sent from any network (see Section 5).

4.5 Circumvention and reselling. You must not circumvent account limits, billing, or usage restrictions; reverse engineer, decompile, or tamper with the Services; or resell, share, or sublicense the Services except as expressly permitted by your plan.

4.6 Abusive infrastructure. You must not operate public anonymising proxies, open relays, or services primarily used to facilitate abuse of third parties from the Services.

5. Email and Anti-Spam

5.1 Consent. Commercial or bulk email may be sent through the Services only to recipients who have given verifiable opt-in consent. You must not use purchased, rented, scraped, or harvested mailing lists.

5.2 Compliance. All email you send must comply with the General Data Protection Regulation, the ePrivacy rules, and any other applicable anti-spam legislation. It must include accurate header and sender information and a working, promptly honoured unsubscribe mechanism.

5.3 Sending limits. To protect deliverability and the reputation of shared mail infrastructure, email sending is subject to per-account and per-server limits. Large or recurring campaigns should be sent using a dedicated mail or newsletter service.

5.4 List hygiene. You are responsible for maintaining the quality of your mailing lists. Sustained high bounce or complaint rates may result in restriction of sending under Section 8.

5.5 No spamvertising. You must not use the Services to host or promote any website or service that is advertised through unsolicited messages sent from any network, regardless of where those messages originate.

6. Resource Usage and Fair Use

6.1 Fair use. Shared hosting and reseller plans operate on a fair-use basis. Your use must not consume resources in a way that degrades the performance, stability, or availability of the Services for other customers, including excessive use of CPU, memory, input/output, processes, database connections, or inodes (file counts).

6.2 Plan limits. The specific resource allowances available to you are defined by your plan specifications and are enforced through account isolation limits (CloudLinux LVE). Sustained overuse may result in throttling, a requirement to upgrade, or suspension in accordance with Section 8.

6.3 Cryptocurrency mining. Cryptocurrency or other digital-asset mining is not permitted on shared hosting, reseller hosting, or managed WordPress plans. It is permitted on VPS and dedicated server plans only, within your plan's resource limits and applicable law.

6.4 Unsuitable workloads. Shared and reseller plans must not be used to operate public file-sharing or torrent trackers, large-scale media streaming, open proxies, or similar resource-intensive services for which those plans are not intended.

Pladinum

7. Security Testing

7.1 Your own applications. You may carry out security or penetration testing only of your own applications hosted on the Services, and only in compliance with this AUP and any instructions we provide.

7.2 Advance notice. You must give at least seven (7) days' notice of the schedule and scope of any such test to security@pladinum.com. This notice is for our monitoring and record-keeping purposes only.

7.3 Load testing. Load or stress testing in any form is permitted only on dedicated servers.

7.4 No testing of our systems. You must not test, probe, or attempt to breach the Pladinum platform, control panels, login or authentication systems, security measures, or any other customer's applications or data. We will not reduce or disable our security measures to accommodate a test.

8. Enforcement and Consequences

8.1 Investigation. We may investigate any suspected, alleged, or actual violation of this AUP, and you agree to cooperate with any such investigation and to take the corrective action we reasonably request. We may cooperate with law enforcement and other authorities and disclose information where required or permitted by law.

8.2 Curable violations. For violations that can be remedied — such as a compromised website, excessive resource use, or an isolated complaint — we will normally notify you and give you a reasonable opportunity, typically between twenty-four (24) and seventy-two (72) hours, to correct the issue. We will restore normal service once the issue has been resolved.

8.3 Immediate action. For violations that are clearly illegal or fraudulent, or that threaten the security, stability, or reputation of the Services, our infrastructure, or other customers — including phishing, malware distribution, active attacks, and child sexual abuse material — we may suspend or terminate the Services immediately and without prior notice.

8.4 Repeat violations. Repeated or persistent violations, including repeat infringement of intellectual property rights, may result in termination of the Agreement.

8.5 Other measures. We may also remove or disable access to offending content, block traffic that we reasonably believe violates this AUP, and take any other action permitted under applicable law. We may recover the reasonable costs of investigating and remedying a violation as provided in the General Terms and Conditions.

8.6 Effect. Suspension or termination resulting from a violation may lead to loss of data and content. Any fees already due remain payable. This Section operates in addition to our rights and remedies under the General Terms and Conditions and at law.

9. Child Sexual Abuse Material

9.1 Zero tolerance. Pladinum has a zero-tolerance policy towards child sexual abuse material ("CSAM"). Any account found to host, store, distribute, or link to such material will be terminated immediately and without notice.

9.2 Preservation and reporting. We will preserve the relevant material and account information as required by law and report it to the competent authorities. No warning or cure period applies to CSAM.

10. Illegal Content Notices and Takedown

10.1 Notice-and-action. Pladinum acts as a hosting intermediary and complies with the EU Digital Services Act and the e-Commerce Directive. If you believe that content hosted on the Services is illegal or infringes your rights, you may submit a notice to abuse@pladinum.com, or to dmca@pladinum.com for copyright matters.

10.2 What to include. A valid notice should identify the specific content or URL, explain the legal basis for the complaint, provide your name and contact details, and include a good-faith statement that the information is accurate.

10.3 Our response. On receiving a valid notice we will act expeditiously and in accordance with the enforcement process in Section 8, which may include notifying the customer, requesting removal within a cure period, or disabling access to the content.

10.4 Customer response. Where appropriate, the affected customer may be given the opportunity to respond to or contest a notice before further action is taken, except where immediate action is required under Section 8.3.

10.5 No general monitoring. Pladinum does not actively monitor the content that customers host and is not obliged to do so. The customer remains solely responsible for their content and Users.

11. Reporting Abuse

11.1 How to report. To report a suspected violation of this AUP, email abuse@pladinum.com. Please include the relevant domain name, IP address, or URL, a description of the issue, and any supporting evidence. For spam reports, please include the complete message headers and body, as these are essential to verify the complaint.

11.2 Handling. We record and investigate all reports. As part of an investigation we may need to verify a report with the customer concerned, and we may disclose a report and related information to that customer for the purpose of resolving the issue. For privacy reasons, we may not be able to share the specific outcome of an investigation with the reporter.

12. Third-Party Services

12.1 The Services may integrate with or provide access to content, software, or services operated by third parties ("Third-Party Services") that are not under Pladinum's control. Your use of any Third-Party Service is at your own risk and is subject to that third party's own terms and privacy policy. Pladinum is not responsible for the availability, performance, or acts or omissions of any Third-Party Service.

13. Customer Responsibilities

13.1 Account security. You are responsible for keeping your account credentials secure, for using strong authentication where available, and for all activity that occurs under your account.

13.2 Maintenance. You are responsible for keeping your applications, content management systems, themes, and plugins updated and patched, and for maintaining your own backups in addition to any backup service we provide.

13.3 Prompt response. You must respond promptly to security and abuse notices from Pladinum, including requests to correct a curable violation under Section 8.2.

14. Changes to this AUP

14.1 We may update this AUP from time to time to reflect changes in our practices, the Services, or legal requirements. Material changes will be communicated through a notice on the Site or by direct notification. Your continued use of the Services after a change takes effect constitutes acceptance of the revised AUP. The "Last revised" date at the top of this document indicates when it was most recently updated.

15. Governing Law

15.1 This AUP is governed by and construed in accordance with the laws of Spain. Any dispute arising from or in connection with this AUP is subject to the jurisdiction provisions set out in the General Terms and Conditions.

16. Contact Information

For questions about this Acceptable Use Policy, or to report abuse, please contact us:

Pladinum Group SL
Avenida Manolete 3a

Pladinum

29660 Marbella, Málaga, Spain
Abuse Reports: abuse@pladinum.com
Copyright / IP Notices: dmca@pladinum.com
Legal: legal@pladinum.com
Customer Portal: my.pladinum.com
Telephone: +34 697 989 840