



Acceptable Use Policy (AUP)

This Acceptable Use Policy ("AUP") describes activities that are not allowed on the Service Provider's network. The AUP is incorporated by reference in the Customer's Agreement with Service Provider herein shall have the meaning given in the Agreement titled 'Cloud Services Agreement'.

1. Abuse. Customer may not use Service Provider's network or Services to engage in, foster, or promote illegal, abusive, or irresponsible behavior, including:

- 1.1 Any activity or conduct that is likely to be in breach of any applicable laws, codes or regulations, including data protection and privacy laws and laws relating to unsolicited commercial electronic messages;
- 1.2 Use of an internet account or computer without the owner's authorization;
- 1.3 Unauthorized access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorization of the owner of the system or network;
- 1.4 Monitoring data or traffic on any network or system without the express authorization of the owner of the system or network;
- 1.5 Introducing intentionally, knowingly or recklessly, any virus or other contaminating code into the Services;
- 1.6 Collecting or using information, including email addresses, screen names or other identifiers, by deceit, (such as, phishing, Internet scamming, password robbery, spidering, and harvesting);
- 1.7 Use of any false, misleading, or deceptive TCP-IP packet header information in an email or a newsgroup posting;
- 1.8 Distributing software that covertly gathers or transmits information about a user;
- 1.9 Distributing advertisement delivery software unless: (i) the user affirmatively consents to the download and installation of such software based on a clear and conspicuous notice of the nature of the software, and (ii) the software is easily removable by use of standard tools for such purpose included on major operating systems (such as Microsoft's "add/remove" tool);
- 1.10 Any conduct that is likely to result in retaliation against the Service Provider network or website, or Service Provider's employees, officers or other agents, including engaging in behavior that results in any server being the target of a denial of service attack (DoS);
- 1.11 Any activity intended to withhold or cloak identity or contact information, including the omission, deletion, forgery or misreporting of any transmission or identification information, such as return mailing and IP addresses;
- 1.12 Interference with service to any user of the Service Provider or other network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks;
- 1.13 Any intentional action which directly or indirectly results in any of our IP space being listed on any abuse database (i.e. Spamhaus);
- 1.14 Conducting any gambling activity in violation of any required licenses, codes of practice, or necessary technical standards required under the laws or regulations of any jurisdiction in which Customer's site is hosted or accessed; or
- 1.15 Any action that is otherwise illegal or solicits conduct that is illegal under laws applicable to the Customer or to Service Provider.
- 1.16 Not store, distribute or transmit any material through the Service that is unlawful, harmful, threatening, defamatory, obscene, harassing or racially or ethnically offensive; facilitates illegal activity; depicts sexually explicit images; promotes unlawful violence, discrimination based on race, gender, color, religious belief, sexual orientation, disability, or any other illegal activities.

2. Offensive Content

Customer may not publish, transmit or store on or via the Services any content or links to any content that Service Provider reasonably believes:

- 2.1 Constitutes, depicts, fosters, promotes or relates in any manner to child pornography, bestiality, any sexual acts, or otherwise unlawfully exploits persons under 18 years of age;
- 2.2 Publish, transmit or store any content or links to any content that is excessively violent, incites violence, threatens violence, contains harassing content or hate speech, creates a risk to a person's safety or health, or public safety or health, compromises national security or interferes with an investigation by law enforcement;

- 2.3. Is unfair or deceptive under the consumer protection laws of any jurisdiction, including chain letters and pyramid schemes;
- 2.4. Is defamatory or violates a person's privacy; or
- 2.5. Is otherwise malicious, fraudulent, morally repugnant.

3. Live Events

Customer may not use its Service Provider services to stream any offensive content (including sexual content), even if the content would otherwise comply with the AUP.

4. No High Risk Use

Customer may not use the Services in any situation where failure or fault of the Services could lead to death or serious bodily injury of any person, or to physical or environmental damage. For example, Customer may not use, or permit any other person to use, the Services in connection with aircraft or other modes of human mass transportation or nuclear or chemical facilities.

5. Vulnerability Testing

Customer may not attempt to probe, scan, penetrate or test the vulnerability of a Service Provider system or network, or to breach the Service Provider security or authentication measures, whether by passive or intrusive techniques. Additionally, the Customer may not perform such testing of its own Hosted System without Service Provider's prior written consent.

6. Export Control

The Services may not be used in violation of export laws, controls, regulations or sanction policies of the applicable jurisdiction. The Services may not be used by persons, organizations, companies or any such other legal entity or unincorporated body, including any affiliate or group company, which is involved with or suspected of involvement in activities or causes relating to: illegal gambling; terrorism; narcotics trafficking; arms trafficking or the proliferation, development, design, manufacture, production, stockpiling, or use of nuclear, chemical or biological weapons, weapons of mass destruction, or missiles; in each case including any affiliation with others whatsoever who sponsor or support the above such activities or causes.

7. Intellectual Property and Other Proprietary Rights

Customer may not use our Services in a manner that infringes on or misappropriates the rights of a third party in any work protected by copyright, trade or service mark, invention, or other intellectual property or proprietary information. For example:

- 7.1 Customer may not use the Services to download, publish, torrent, distribute, use, or otherwise copy in any manner any text, music, software, art, image, or other work protected by copyright law unless the Customer has permission from the owner of the work to use or copy the work in that manner, or the Customer is otherwise permitted by established intellectual property law to copy or use the work or rights in that manner;
- 7.2 Customer may not use the Services to publish content intended to assist others in defeating technical copyright protections; and
- 7.3 Customer may not display another person's trademark without permission.
- 7.4 In addition, Customer may not use the Services to publish another person's trade secrets, or to publish information in violation of a duty of confidentiality. It is Service Provider's policy to terminate the services of customers who are repeat infringers in appropriate circumstances.

8. Cooperation with Investigations and Legal Proceedings

If we are legally required to permit any relevant authority to inspect the Customer content or traffic, the Customer agrees we can do so; provided however that, where possible without breaching any legal or regulatory requirement, we give the Customer reasonable prior written notice of such requirement.

We may, without notice to the Customer, report to the appropriate authorities any conduct by the Customer that we believe violates applicable law, and provide any information we have about the Customer, or its users or its traffic and cooperate in response to a formal request from a law enforcement or regulatory agency investigating any such activity, or in response to a formal request in a civil action that on its face meets the requirements for such a request.



9. Excessive Use of Shared System Resources

Customer may not use any shared system provided by Service Provider in a way that unnecessarily interferes with the normal operation of the shared system, or that consumes a disproportionate share of the resources of the system. For example, we may require the Customer to repair coding abnormalities in its Cloud-hosted code if it unnecessarily conflicts with other Cloud customers' use of the Cloud.

10. Third Party Conduct

Customer is responsible for violations of this AUP by anyone with the Customer's permission or on an unauthorized basis as a result of the Customer's failure to use reasonable security precautions.

The Customer's use of the Services to assist another person in an activity that would violate this AUP if performed by the Customer is a violation of the AUP.

Customer must use reasonable efforts to secure any device or network within its control against being used in breach of the applicable laws against spam and unsolicited email, including where appropriate by the installation of antivirus software, firewall software and operating system and application software patches and updates. Our right to suspend or terminate the Service applies even if a breach is committed unintentionally or without the Customer's authorization, including through a Trojan horse or virus.

11. Other

- 11.1 Customer must have valid and current information on file with its domain name registrar for any domain hosted on the Service Provider network.
- 11.2 Customer may only use IP addresses assigned to the Customer by Service Provider in connection with its Service Provider services.
- 11.3 Customer agree that if the Customer register a DNS record or zone on Service Provider managed or operated DNS servers or services for a domain of which the Customer are not the registrant or administrative contact according to the registrars WHOIS system, that, upon request from the registrant or administrative contact according to the registrars WHOIS system, Service Provider may modify, transfer, or delete such records or zones.
- 11.4 Customer may not register to use any Services under a false name, or use an invalid or unauthorized credit card in connection with any Services.

12. Changes to the AUP

The Internet is still evolving, and the ways in which the Internet may be abused are also still evolving. Therefore, we may from time to time amend this AUP to further detail or describe reasonable restrictions on the Customer's use of our Services by publishing a revised version of the AUP, or in the event of a material adverse change to the AUP, by providing you thirty (30) days written notice.

The revised AUP will become effective as to you on the first to occur of: (i) the Customer's execution of a new or additional agreement for all or part of its Hosted System that incorporates the revised AUP by reference, (ii) the first day of a renewal term for an Agreement that begins at least thirty (30) days after the time that the revised AUP has been posted, or (iii) thirty (30) days following our written notice to the Customer of a material change to the AUP.

If Customer's compliance with the revised AUP would adversely affect its use of the Hosting Services, the Customer may elect to terminate the Agreement by giving Service Provider written notice of its objection no later than thirty (30) days following the date that the revised AUP would otherwise have become effective to the Customer. Service Provider will not charge the Customer an early termination fee for a termination on these grounds. If the Customer elect to terminate, the Customer may continue using the Services for up to an additional ninety (90) days and we will not enforce the revision to the Customer during this time, Customer will continue to be subject to the prior version. If the Customer choose to terminate the Services under this Subsection, we may decide to waive that change applicable to the Customer and keep the Agreement in place for the remainder of the term.

13. Consequences of Violation of AUP

If the Customer breach the AUP we may suspend or terminate the Services in accordance with the Agreement. We may intercept or block any content or traffic belonging to the Customer or to users where Services are being used unlawfully or not in accordance with this AUP.

No credit will be available under the Service Provider Service Level Agreement for interruptions of service resulting from any AUP violation.

14. Right to Appeal and Dispute Resolution

In case of an AUP violation notice, Customer has 3 business days to appeal in writing, detailing why the assessment is incorrect and proposing a resolution. Service Provider will review and provide a final decision within 7 days. If unsatisfied, Customer can initiate dispute resolution steps under relevant of Cloud Service Agreement. During appeal/dispute resolution, Service Provider at its own discretion may withhold suspension unless posing a direct security threat.