

ACCEPTABLE USE POLICY

Introduction

By using any of our services, you agree to comply with this AUP and to remain responsible for your users, where applicable. We reserve the right to change or modify the terms of the AUP at any time, by posting an updated version on our website at www.liquidcloud.co.za. Your use of our services after changes to the AUP are posted shall constitute acceptance of any changed or additional terms.

Scope of the AUP

The AUP applies to all of our services including Internet services, including but not limited to hosting services (data/content hosting, server hosting, web hosting, etc) or any other services provided over the Internet or wireless data networks (collectively "IP Services").

Prohibited Activities

General Prohibitions: We prohibit the use of the IP Services in any way that is: i) unlawful, incitement to commit criminal acts, harmful to or interferes with use of our network or systems; ii) interferes with the use or enjoyment of services received by others; iii) infringes intellectual property rights; iv) results in the publication of threatening or offensive material which is harmful, obscene, discriminatory, defamatory, constitutes hate speech; or v) constitutes abuse, a security risk or a violation of privacy.

Unlawful Activities: IP Services shall not be used in connection with any criminal, civil or administrative violation of any applicable local, provincial, national or international law, treaty, court orders, ordinance, regulation or administrative rules.

Violation of Intellectual Property Rights: IP Service(s) shall not be used to publish, submit/receive upload/download, post, use, copy or otherwise reproduce, transmit, re-transmit, distribute or store any content/material or to engage in any activity that infringes, misappropriates or otherwise violates the intellectual property rights or privacy or publicity rights of any individual, group or entity, including but not limited to any rights protected by any copyright, patent, trademark laws, trade secret, trade dress, right of privacy, right of publicity, moral rights or other intellectual property right now known or later recognized by statute, judicial decision or regulation.

Threatening Material or Content: IP Services shall not be used to host, post, transmit, or re-transmit any content or material (or to create a domain name or operate from a domain name), that harasses, or threatens the health or safety of others. In addition, for those IP Services that utilize our content hosting, We reserve the right to decline to provide such services if the content is determined by us to be obscene, indecent, hateful, malicious, racist, defamatory, fraudulent, libelous, treasonous, excessively violent or promoting the use of violence or otherwise harmful to others.

Inappropriate Interaction with Minors: IP Services should not be used for the purpose of commission an offence against a child or in way that would constitute or promote unlawful interaction with children.

Child Pornography: IP Services shall not be used to publish, submit/receive, upload/download, post, use, copy or otherwise produce, transmit, distribute or store child pornography. Suspected violations of this prohibition may be reported to us at the following e-mail address: info@liquidcloud.co.za. We will report any discovered violation of this prohibition to the South African Police services and take steps to remove child pornography (or otherwise block access to the content determined to contain child pornography) from our servers.

Spam/E-mail Abuse:

Spam/E-mail abuse is prohibited using IP Services. Spam/E-mail abuse shall include, but are not limited to, the following activities:

- sending multiple unsolicited electronic mail messages or "mail-bombing" to one or more recipient;
- sending unsolicited commercial e-mail, or unsolicited electronic messages directed primarily at the advertising or promotion of products or services;
- sending unsolicited electronic messages with petitions for signatures or requests for charitable donations, or sending any chain mail related materials;
- sending bulk electronic messages without identifying, within the message, a reasonable means of opting out from receiving additional messages from the sender;
- sending electronic messages, files or other transmissions that exceed contracted for capacity or that create the potential for disruption of our network or of the networks with which we interconnect, by virtue of quantity, size or otherwise;
- using another site's mail server to relay mail without the express permission of that site;
- using another computer, without authorization, to send multiple e-mail messages or to retransmit e-mail messages for the purpose of misleading recipients as to the origin or to conduct any of the activities prohibited by this AUP;
- using IP addresses that you do not have a right to use;
- collecting the responses from unsolicited electronic messages;
- maintaining a site that is advertised via unsolicited electronic messages, regardless of the origin of the unsolicited electronic messages;
- sending messages that are harassing or malicious, or otherwise could reasonably be predicted to interfere with another party's quiet enjoyment of the IP Services (e.g., through language, frequency, size or otherwise);
- using distribution lists containing addresses that include those who have opted out;
- sending electronic messages that do not accurately identify the sender, the sender's return address, the e-mail address of origin, or other information contained in the subject line or header;
- falsifying packet header, sender, or user information whether in whole or in part to mask the identity of the sender, originator or point of origin;
- using redirect links in unsolicited commercial e-mail to advertise a website or service;
- posting a message to more than ten (10) online forums or newsgroups, that could reasonably be expected to generate complaints;
- intercepting, redirecting or otherwise interfering or attempting to interfere with e-mail intended for third parties;

- knowingly deleting any author attributions, legal notices or proprietary designations or labels in a file that the user mails or sends;
- using, distributing, advertising, transmitting, or otherwise making available any software program, product, or service that is designed to violate this AUP or the AUP of any other Internet Service Provider, including, but not limited to, the facilitation of the means to spam.

Security Violations

Customers are responsible for ensuring and maintaining security of their systems and the machines that connect to and use IP Service(s), including implementation of necessary patches and operating system updates.

IP Services may not be used to interfere with, gain unauthorized access to, or otherwise violate the security of our (or another party's) server, network, network access, personal computer or control devices, software or data, or other system, or to attempt to do any of the foregoing. System or network security violations shall include, but are not limited to:

- unauthorized monitoring, scanning or probing of network or system or any other action aimed at the unauthorized interception of data or harvesting of e-mail addresses;
- hacking, attacking, gaining access to, breaching, circumventing or testing the vulnerability of the user authentication or security of any host, network, server, personal computer, network access and control devices, software or data without express authorization of the owner of the system or network;
- impersonating others or secretly or deceptively obtaining personal information of third parties (phishing, etc.);
- using any program, file, script, command or transmission of any message or content of any kind, designed to interfere with a terminal session, the access to or use of the Internet or any other means of communication;
- distributing or using tools designed to compromise security (including but not limited to SNMP tools), including cracking tools, password guessing programs, packet sniffers or network probing tools (except in the case of authorized legitimate network security operations);
- knowingly uploading or distributing files that contain viruses, spyware, Trojan horses, worms, time bombs, cancel bots, corrupted files, root kits or any other similar software or programs that may damage the operation of another's computer, network system or other property, or be used to engage in modem or system hi-jacking;
- engaging in the transmission of pirated software;
- with respect to dial-up accounts, using any software or device designed to defeat system time-out limits or to allow Customer's account to stay logged on while Customer is not actively using the IP Services or using such account for the purpose of operating a server of any type;
- using manual or automated means to avoid any use limitations placed on the IP Services;
- providing guidance, information or assistance with respect to causing damage or security breach to our network or systems, or to the network of any other IP Service provider;

- failure to take reasonable security precautions to help prevent violation(s) of this AUP.

Customer Responsibilities

Customers remain solely and fully responsible for the content of any material posted, hosted, downloaded/uploaded, created, accessed or transmitted using the IP Services. We have no responsibility for any material accessible using IP Services.

Customers are responsible for taking prompt corrective action(s) to remedy a violation of AUP and to help prevent similar future violations.

AUP Enforcement and Notice

Customer's failure to observe the guidelines set forth in this AUP may result in us taking actions, which may either be a warning, a suspension or termination of Customer's IP Services.

If the IP Services are used in a way that we, in our sole discretion, believe violates this Acceptable Use Policy or any of our rules or limitations, we may take any responsive actions we deem appropriate.

Should you engage in any one or more of the above activities, which shall be determined in our sole discretion and which decision shall be final, then we shall be entitled, without prejudice to any other rights we may have, to take any responsive action we deem appropriate, such actions may include, without limitation:

- without notice, temporary or permanent limitation, restriction or suspension of your access to the IP Service concerned;
- terminate all agreements with you with immediate effect; and
- disclose information relating to the offending activity as may be required under the circumstances.

We have no obligation to monitor content of any materials distributed or accessed using the IP Services. However, we may monitor content of any such materials as necessary to comply with applicable laws, regulations or other governmental or judicial requests; or to protect the our network and our customers.

Incident Reporting

Any complaints (other than claims of copyright or trademark infringement) regarding violation of this AUP by a Customer (or its user) should be directed to info@liquidcloud.co.za and include details that would assist us in investigating and resolving such complaint.