Acceptable Use Policy

This Policy forms part of the Agreement between the Client and WMP Host and is binding on Clients using WMP Host's services. The AUP sets out in detail what forms of conduct WMP Host regards as unacceptable on the part of its Clients and the steps which WMP Host may take in response to unacceptable use of its services. Please take the time to acquaint yourself fully with the provisions of this Policy.

1. General

1.1 By contracting with WMP Host for services, the Client agrees, without limitation or qualification, to be bound by this Policy and the terms and conditions it contains, as well as any other additional terms, conditions, rules or policies which are displayed to the Client in connection with the Services.

1.2 The purpose of this AUP is to:

1.2.1 ensure compliance with the relevant laws of the Republic;

1.2.2 specify to Clients and users of WMP Host's service what activities and online behaviour are considered an unacceptable use of the service;

1.2.3 protect the integrity of WMP Host's network; and

1.2.4 specify the consequences that may flow from undertaking such prohibited activities.

1.3 This document contains a number of legal obligations which the Client will be presumed to be familiar with. As such, WMP Host encourages the Client to read this document thoroughly and direct any queries to aup@wmphost.net.

1.4 WMP Host respects the rights of WMP Host's Clients and users of WMP Host's services to freedom of speech and expression, access to information, privacy, human dignity, religion, belief and opinion.

2. Unacceptable Use

2.1 WMP Host's services may only be used for lawful purposes and activities. WMP Host prohibits any use of its Services including the transmission, storage and distribution of any material or content using WMP Host's network that violates any law or regulation of the Republic. This includes, but is not limited to:

2.1.1 Any violation of local and international laws prohibiting child pornography, obscenity, discrimination (including racial, gender or religious slurs) and hate speech, or speech designed to incite violence or hatred, or threats to cause bodily harm.

2.1.2 Any activity designed to defame, abuse, stalk, harass or physically threaten any individual in the Republic or beyond its borders; including any attempt to link to, post, transmit or otherwise distribute any inappropriate or defamatory material.

2.1.3 Any violation of Intellectual Property laws including materials protected by local and international copyright, trademarks and trade secrets.

2.1.4 Any violation of another's right to privacy, including any effort to collect personal data of third parties without their consent.

2.1.5 Any fraudulent activity whatsoever, including dubious financial practices, such as pyramid schemes; the impersonation of another client without their consent; or any attempt to enter into a transaction with WMP Host on behalf of another client without their consent.

2.1.6 Any violation of the exchange control laws of the Republic.

2.1.7 Any activity that results in the sale, transmission or distribution of pirated or illegal software.

3. Threats to Network Security

3.1 Any activity which threatens the functioning, security and/or integrity of WMP Host's network is unacceptable. This includes:

3.1.1 Any efforts to attempt to gain unlawful and unauthorised access to the network or circumvent any of the security measures established by WMP Host for this goal.

3.1.2 Any effort to use WMP Host's equipment to circumvent the user authentication or security of any host, network or account ("cracking" or "hacking").

3.1.3 Forging of any TCP/IP packet headers (spoofing) or any part of the headers of an email or a newsgroup posting.

3.1.4 Any effort to breach or attempt to breach the security of another user or attempt to gain access to any other person's computer, software, or data without the knowledge and consent of such person.

3.1.5 Any activity which threatens to disrupt the service offered by WMP Host through "denial of service attacks"; flooding of a network, or overloading a service or any unauthorised probes ("scanning" or "nuking") of others' networks.

3.1.6 Any activity which in any way threatens the security of the network by knowingly posting, transmitting, linking to or otherwise distributing any information or software which contains a virus, trojan horse, worm, malware, botnet or other harmful, destructive or disruptive component.

3.1.7 Any unauthorised monitoring of data or traffic on the network without WMP Host's explicit, written consent.

3.1.8 Running services and applications with known vulnerabilities and weaknesses, e.g. insufficient anti-automation attacks, any traffic amplification attacks, including recursive DNS attacks, SMTP relay attacks.

3.1.9 Failing to respond adequately to a denial-of-service attack (DOS / DDOS).

4.Contention

4.1 Network capacity and performance is subject to contention for services from users. This means that a significant rise in demand can affect the availability of bandwidth to users. WMP Host manages contention through the implementation of Quality of Service, Shaping and Throttling (on applicable products). Contention is a function of demand from users and is not strictly within WMP Host's direct control, however WMP Host will use the provisions of the AUP and Terms and Conditions to manage contention and minimise the impact to performance to offer the best possible experience at all times.

5. Spam and Unsolicited Bulk Mail

5.1 WMP Host regards all unsolicited bulk email (whether commercial in nature or not) as spam, with the following exceptions:

5.1.1 Mail sent by one party to another where there is already a prior relationship between the two parties and the subject matter of the message(s) concerns that relationship;

5.1.2 Mail sent by one party to another with the explicit consent of the receiving party.

5.1.3 Clients should only receive bulk mail that they have requested and/or consented to receive and/or which they would expect to receive as a result of an existing relationship.

5.2 WMP Host will take swift and firm action against any user engaging in any of the following unacceptable practices:

5.2.1 Sending unsolicited bulk mail for marketing or any other purposes (political, religious or commercial) to people who have not consented to receiving such mail.

5.2.2 Using any part of WMP Host's infrastructure for the purpose of unsolicited bulk mail, whether sending, receiving, bouncing, or facilitating such mail.

5.2.3 Operating or maintaining mailing lists without the express permission of all recipients listed. In particular, WMP Host does not permit the sending of "opt-out" mail, where the recipient must opt out of receiving mail which they did not request. For all lists, the sender must maintain meaningful records of when and how each recipient requested mail. WMP Host will also monitor Clients deemed to be operating "cleaning lists", which is using illegally obtained email addresses but removing addresses as complaints arise. Should WMP Host, at its discretion, believe that this is the case, it will be treated as SPAM.

5.2.4 Failing to promptly remove from lists invalid or undeliverable addresses or addresses of unwilling recipients or a recipient who has indicated s/he wishes to be removed from such list, or failing to provide the recipient with a facility to opt-out.

5.2.5 Using WMP Host's service to collect responses from unsolicited email sent from accounts on other Internet hosts or e-mail services that violate this AUP or the AUP of any other Internet service provider. Advertising any facility on WMP Host's infrastructure in unsolicited bulk mail (e.g. a website advertised in spam).

5.2.6 Including WMP Host's name in the header or by listing an IP address that belongs to WMP Host in any unsolicited email whether sent through WMP Host's network or not.

5.2.7 Failure to secure a Client's mail server against public relay as a protection to themselves and the broader Internet community. Public relay occurs when a mail server is accessed by a third party from another domain and utilised to deliver mails, without the authority or consent of the owner of the mail-server. Mail servers that are unsecured against public relay often become abused by unscrupulous operators for spam delivery and upon detection such delivery must be disallowed. WMP Host reserves the right to examine users' mail servers to confirm that no mails are being sent from the mail server through public relay and the results of such checks can be made available to the user. WMP Host also reserves the right to examine the mail

servers of any users using WMP Host's mail servers for "smarthosting" (when the user relays its mail via an WMP Host mail server to a mail server of its own or vice versa) or similar services at any time to ensure that the servers are properly secured against public relay. All relay checks will be done in strict accordance with WMP Host's Privacy Policy and the laws of South Africa.

6. Users Outside of South Africa

6.1 Where any user resides outside of the Republic, permanently or temporarily, such user will be subject to the laws of the country in which s/he is currently resident and which apply to the user. On presentation of a legal order to do so, or under obligation through an order for mutual foreign legal assistance, WMP Host will assist foreign law enforcement agencies (LEAs) in the investigation and prosecution of a crime committed using WMP Host's resources, including the provisioning of all personal identifiable data.

7. Hosting

7.1 WMP Host offers unlimited bandwidth (web traffic) usage on Shared Hosting platforms. However, this is subject to reasonable and responsible usage, as determined at WMP Host's discretion. Shared Hosting is designed for serving personal hosting requirements or that of small enterprises, and not medium to large enterprises. WMP Host reserves the right to move Clients deemed to have excessive bandwidth usage to a Cloud product, which will better suit their requirements. Clients will be given notice as such, and will be informed of any cost implications.

7.2 Disk Space on Shared Hosting may only be used for Website Content, Emails and related System Files. General data storage, archiving or file sharing of documents, files or media not directly related to the website content is strictly prohibited. Unauthorised storage or distribution of copyrighted materials is prohibited, via FTP hosts or any other means.

7.3 For Shared Hosting and Managed Dedicated Solutions, WMP Host will implement security updates, software patches and other updates or upgrades from time to time, to maintain the best performance, at their sole discretion. These upgrades include, but are not limited to, PHP, MySQL and CPanel release versions. WMP Host is under no obligation to effect such upgrades, or to rectify any impact such changes could potentially have to Hosting Clients.

7.4 WMP Host will not be liable or responsible for the backing up, restoration or loss of data under any circumstances. Clients are solely responsible for ensuring their data is regularly backed up and for restoring such backups in the event of data loss or corruption.

7.5 WMP Host prohibits Clients from doing the following on hosting platforms administered by WMP Host:

7.5.1 Running applications that are not production-ready. Any applications on the hosting platform must be optimised with respect to memory usage and must have appropriate data indexing.

7.5.2 Running applications with inadequate security controls.

7.5.3 Generating significant side-channel traffic from an application, whether by design or otherwise. Databases should be stored locally, and remote content should be cached.

7.5.4 Failure to maintain proper "housekeeping" on a shared server including storing or generating useless content, including comment spam, unused cache files, log file and database entries.

7.5.5 Storing malicious content, such as malware or links to malware.

7.5.6 Monopolising server resources, including CPU time, memory, network and disk bandwidth.

7.5.7 Maintaining long-running processes and long-running database queries.

7.5.8 Storing or running back-door shells, mass mailing scripts, proxy servers, web spiders, phishing content, or peer-to-peer software.

7.5.9 Sending bulk mail of any form, particularly mail that cannot be efficiently delivered due to volume or incorrect addresses.

7.5.10 Using poor passwords.

7.5.11 Sharing security credentials with untrusted parties.

7.5.12 Running Torrents for download or Seed Servers.

7.5.13 Running TOR (or other Online Anonymity Services).

7.5.14 Otherwise circumventing the Acceptable Use Policy or intended use of the product.

7.6 WMP Host strictly prohibits any crypto currency associated activities or mechanisms to be run on any part of our hosting network or servers within our hosting environment.

8. Protection of Minors

8.1 WMP Host prohibits Clients from using WMP Host's service to harm or attempt to harm a minor, including, but not limited to, by hosting, possessing, disseminating, distributing or transmitting material that is unlawful, including child pornography and cyber bullying.

8.2 WMP Host prohibits Clients from using WMP Host's service to host sexually explicit or pornographic material of any nature.

9. Privacy and Confidentiality

9.1 WMP Host respects the privacy and confidentiality of WMP Host's Clients and users of WMP Host's service. Please review WMP Host's Privacy Policy which details how WMP Host collects and uses personal information gathered in the course of operating its Services.

10. User Responsibilities

10.1 Clients are responsible for any misuse of WMP Host's services that occurs through the Client's account. It is the Client's responsibility to ensure that unauthorised persons do not gain access to or misuse WMP Host's service.

10.2 WMP Host urges Clients not to reply to unsolicited mail or "spam", not to click on any suggested links provided in the unsolicited mail. Doing so remains the sole responsibility of the Client and WMP Host cannot be held liable for the Client being placed on any bulk mailing lists as a result.

10.3 Where the Client has authorised a minor to use any of the WMP Host's services or access its websites, the Client accepts that as the parent/legal guardian of that minor, the Client is

fully responsible for: the online conduct of such minor, controlling the minor's access to and use of any services or websites, and the consequences of any misuse by the minor.

11. Complaints Procedure

11.1 Complaints relating to the violation of this AUP should be submitted in writing to abuse@wmphost.net. Complaints must be substantiated, and unambiguously state the nature of the problem, and its connection to WMP Host's network and services.

12. Action Following Breach of the AUP

12.1 Upon receipt of a complaint, or having become aware of an incident, WMP Host may, in its sole and reasonably-exercised discretion take any of the following steps:

- 12.1.1 In the case of Clients, warn the Client, suspend the Client account and/or revoke or cancel the Client's Service access privileges completely;
- 12.1.2 In the case of an abuse emanating from a third party, inform the third party's network administrator of the incident and request the network administrator or network owner to address the incident in terms of this AUP and/or the ISPA Code of Conduct (if applicable);
- 12.1.3 In severe cases suspend access of the third party's entire network until abuse can be prevented by appropriate means;
- 12.1.4 In all cases, charge the offending parties for administrative costs as well as for machine and human time lost due to the incident;
- 12.1.5 Assist other networks or website administrators in investigating credible suspicions of any activity listed in this AUP;
- 12.1.6 Institute civil or criminal proceedings;
- 12.1.7 Share information concerning the incident with other Internet access providers, or publish the information, and/or make available the users' details to law enforcement agencies; and/or
- 12.1.8 suspend or terminate the Service as provided for in the Agreement.

12.2 This policy applies to and will be enforced for intended and unintended (e.g., viruses, worms, malicious code, or otherwise unknown causes) prohibited usage.

13. Reservation and Non-Waiver of Rights

13.1 WMP Host reserves the right to amend or alter this policy at any time, and without notice to the Client.

13.2 WMP Host reserves the right to take action against any individuals, companies or organisations that violate the AUP, or engage in any illegal or unlawful activity while accessing WMP Host's services, to the fullest extent of the law.

13.3 WMP Host reserves the right, at its sole discretion, to act against other types of abuse not listed in this document and to investigate or prevent illegal activities being committed over WMP Host's network.

13.4 WMP Host does not waive its right to enforcement of this AUP at any time, or prejudice its right to take subsequent action, should WMP Host fail, neglect or elect not to enforce a breach of the AUP at any time.