1. General

1.1. By contracting with Wiza Solutions 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 Wiza Solutions's service what activities and online behaviour are considered an unacceptable use of the service;

1.2.3. protect the integrity of Wiza Solutions'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, Wiza Solutions encourages the Client to read this document thoroughly and direct any queries to aup@getwiza.com

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

2. Unacceptable Use

2.1. Wiza Solutions's services may only be used for lawful purposes and activities. Wiza Solutions prohibits any use of its Services including the transmission, storage and distribution of any material or content using Wiza Solutions'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 Wiza Solutions 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 Wiza Solutions'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 Wiza Solutions for this goal.

3.1.2. Any effort to use Wiza Solutions'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 Wiza Solutions 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 Wiza Solutions'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. Definitions

4.1. Shaping

4.1.1. Shaping is the implementation of protocol based priority, to manage demand on the network. When shaping is implemented, realtime, interactive services are given higher priority over non-realtime, non-interactive services, effectively slowing the performance of non-prioritised services in favour of those given priority. Shaping is applied to all users in general (not based on usage thresholds), and the impact to non-priority services is determined by the level of demand and available network capacity. Shaping is applied only when demand on the network exceeds available network capacity, and relieved when demand decreases.

4.2. Throttling

4.2.1.Throttling limits the throughput of all services and protocols. Regardless of the DSL line speed, a throttled account will only be able to achieve limited throughput in total whilst using that account on their line. The DSL line itself is not affected, and using an unthrottled account will return line performance to normal. throttling is applied on an individual user basis, based on usage over a 30 day rolling window threshold. Throttling is applied only when demand on the network exceeds available network capacity, and is relieved when demand decreases.

5. Uncapped Fibre

5.1. Uncapped Fibre Services are intended for home and personal use. Reselling services or use of home services for business purposes are prohibited.

5.2. 7.2Uncapped Fibre may not be used to provide or resell services to other indivudals, and this is prohibited in the following scenarios (but not limited):

5.2.1. Wireless Internet Service Provision

5.2.2.Hosting Shell Accounts

5.2.3.Providing email, news, download, VPN or sandbox services

5.2.4.Running of home servers or private servers

5.2.5.Provision of network services to others

5.2.6.Running private servers for mail, HTTP, FTP, IRC and multi-user forums

5.3. Services may not be shared

6. Contention

6.1. 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. Wiza Solutions 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 Wiza Solutions's direct control, however Wiza Solutions 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.

7. Spam and Unsolicited Bulk Mail

7.1. Wiza Solutions regards all unsolicited bulk email (whether commercial in nature or not) as spam, with the following exceptions:

7.1.1. 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;

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

7.1.3. 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.

7.2. Wiza Solutions will take swift and firm action against any user engaging in any of the following unacceptable practices:

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

7.2.2. Using any part of Wiza Solutions’s infrastructure for the purpose of unsolicited bulk mail, whether sending, receiving, bouncing, or facilitating such mail.

7.2.3. Operating or maintaining mailing lists without the express permission of all recipients listed. In particular, Wiza Solutions 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. Wiza Solutions will also monitor Clients deemed to be operating “cleaning lists”, which is using illegally obtained email addresses but removing addresses as complaints arise. Should Wiza Solutions, at its discretion, believe that this is the case, it will be treated as SPAM.

7.2.4. 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.

7.2.5. Using Wiza Solutions'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 Wiza Solutions’s infrastructure in unsolicited bulk mail (e.g. a website advertised in spam).

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

7.2.7. 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. Wiza Solutions 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. Wiza Solutions also reserves the right to examine the mail servers of any users using Wiza Solutions's mail servers for "smarthosting" (when the user relays its mail via an Wiza Solutions 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 Wiza Solutions's Privacy Policy and the laws of South Africa.

8. Users Outside South Africa

8.1. 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, Wiza Solutions will assist foreign law enforcement agencies (LEAs) in the investigation and prosecution of a crime committed using Wiza Solutions's resources, including the provisioning of all personal identifiable data.

9. Protection of Minors

9.1. Wiza Solutions prohibits Clients from using Wiza Solutions'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.

9.2. Wiza Solutions prohibits Clients from using Wiza Solutions’s service to host sexually explicit or pornographic material of any nature.

10. Privacy and Confidentiality

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

11. User Responsibilities

11.1. Clients are responsible for any misuse of Wiza Solutions'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 Wiza Solutions's service.

11.2. Wiza Solutions 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 Wiza Solutions cannot be held liable for the Client being placed on any bulk mailing lists as a result.

11.3. Where the Client has authorised a minor to use any of the Wiza Solutions'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.

12. Action Following Breach of the AUP

12.1. Upon receipt of a complaint, or having become aware of an incident, Wiza Solutions 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.