ANNEXURE 8 – ACCEPTABLE USE POLICY

PREAMBLE

Customer agrees, without limitation or qualification, to be bound by this policy and the term and conditions it contains, as well as any other additional terms, conditions, rules or policies or amendments from time to time, available at eoh-ns.co.za and which amendments will be supplied to the Customer by the Service Provider.

ACCEPTABLE USE POLICY

The purpose of this Acceptable Use Policy (AUP) is to comply with the relevant laws of the Republic of South Africa, including the terms and conditions of use of the MNS (as defined in the Managed Network Services Agreement); to specify to Clients and users of our service/website what activities and online behaviour are considered an unacceptable use of the service/website; to protect the integrity of our network and to specify the consequences that may flow from undertaking such prohibited activities.

This document contains a number of legal obligations which you are presumed to be familiar with. As such, we encourage you to read this document thoroughly and direct any queries to our Customer services/legal department at 0860 88 0860.

The Service Provider respect the rights of our Customers and users of our services to freedom of speech and expression; access to information; privacy; human dignity; religion; belief and opinion in accordance with our constitution. We undertake not to interfere with any of those rights unless required to do so by law; unless those rights are exercised for unlawful purposes; or unless the exercise of those rights threatens to cause harm to another person or affect the integrity of our network.

ISPA membership and Code of Conduct

The Service Provider confirms that in compliance with section 72 of the Electronic Communications and Transactions Act 25 of 2002, The Service Provider is a member of the Internet Service Providers' Association (ISPA) and has adopted and implemented the association's official Code of Conduct, which can be viewed at http://www.ispa.org.za code.

Unlawful Use

The Service Provider's services/website may only be used for lawful purposes and activities. We prohibit any use of our website/network including the transmission, storage and distribution of any material or content using our network that violates any law or regulation of the Republic. This includes:

- 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.
- 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.
- Any violation of the individual's right to privacy, including any effort to collect personal data of third parties without their consent.
- Any fraudulent activity whatsoever, including dubious financial practices, such as pyramid schemes; the impersonation of another subscriber without their consent; or any attempt to enter into a transaction with The Service Provider on behalf of another subscriber without their consent.
- Any violation of the exchange control laws of the Republic.
- Any activity that results in the sale, transmission or distribution of pirated or illegal software.
- Failing to respond to a request be a recipient of unsolicited mail to be removed from any mailing or direct marketing list and continuing to send unsolicited mail following such a request for removal.

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. On presentation of a legal order to do so, or under obligation through an order for mutual foreign legal assistance, The Service Provider will assist foreign law enforcement agencies (LEA) in the investigation and prosecution of a crime committed using The Service Provider's resources, including the provisioning of all personal identifiable data.

Prohibited Activities

The following sections outline activities that are considered an unacceptable us of the Service Provider's services/network/website and also detail the guidelines for acceptable use of certain facilities/services, as the case may be.

Threats to Network Security

Any activity which threatens the functioning security and/or integrity of the Service Provider network is unacceptable. This includes:

- Any efforts to attempt to gain unlawful and unauthorised access to the network or circumvent any of the security measures established by the Service Provider for this goal;
- Any effort to use the Service Provider equipment to circumvent the user authentication or security of any host, network or account ("cracking" or "hacking");
- Forging of any TCP-IP packet header (spoofing) or any part of the header information in an email or a newsgroup posting;
- 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;
- Any activity which threatens to disrupt the service offered by the Service Provider through "denial of service attacks'' flooding of a network, or overloading a service or any unauthorised probes ("scanning' or "nuking") of others' networks;
- 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, lock, mail bomb or other harmful, destructive or disruptive component;
- Any unauthorised monitoring of data or traffic on the network without the Service Provider's explicit, written consent;
- Any unsolicited mass mailing activity including direct marketing spam and chain letters for commercial or other purposes, without the consent of the recipients of those mails.

Public Space and Third Party Content and sites

In reading this AUP or in signing a service contract with the Service Provider, you acknowledge that the Service Provider has no power to control the content of the information passing over the Internet and its applications, including e-mail; chat rooms; news groups; or other similar for a, and that the Service Provider cannot be held responsible or liable, directly or indirectly, for any of the abovementioned content, in any way for any loss or damage of any kind incurred as a result of, or in connection with your use of, or reliance on, any such content.

Our services also offer access to numerous third party web pages. You acknowledge that we exercise absolutely no control over such third party content, or sites and in such cases, our network is merely a conduit or means of access and transmission. This includes but is not limited to, third party content contained on or accessible through the Service Provider's network websites and web pages or sites displayed as search results or contained within directory of links on the Service Provider network. It remains your responsibility to review and evaluate any such content, and that any and all risk associated.

Access to public Internet spaces, such as bulletin boards, Usenet groups, chat rooms and moderated forums is entirely voluntary and at your own risk.

The Service Provider employees do not moderate any of these services, or your communications, transmissions or use of these services. We do not undertake any responsibility for any content contained therein, or for any breaches of your right to privacy that you may experience as a result of accessing such spaces.

Unsolicited, Spam and Junk mail

Spam and unsolicited bulk mail are highly problematic practices. They affect the use and enjoyment of services by others and often compromise network security. The Service Provider will take swift and firm action against any user engaging in any of the following unacceptable practices:

- Sending unsolicited bulk mail for marketing or any other purposes (political, religious or commercial) to people who have not consented to receiving such mail;
- Operating or maintaining mailing lists without the express permission of all recipients listed;
- Failing to promptly remove from lists invalid or undeliverable addresses or addresses of unwilling recipients;
- Using the Service Provider's services to collect responses from unsolicited email send from accounts on other Internet hosts or email services, that violate this AUP or the AUP of any other Internet service provider;
- Including the Service Provider's name in the header or by listing an IP address that belongs to the Service Provider in any unsolicited email sent through the Service Provider's network or not;
- Failure to secure a Customer'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 of consent of the owner of the mail-server. Mail servers that are unsecured against public relay often become abused by unscrupulous operators from spam delivery and upon detection such delivery must be disallowed. The Service Provider 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. The Service Provider also reserves the right to examine the mail servers of any users using the Service Provider's mail servers for "smarthosting" (when the user relays its mail via the Service Provider's mail server to a mail server of its own) 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 the Service Provider's privacy policy.

Protection of Minors

The Service Provider prohibits Customers from using its 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.

Privacy and Confidentiality

The Service Provider respects the privacy and confidentiality of our Customers and users of our services. Please review our policy which details how we collect and use personal information gathered in the course of operating this service.

User Responsibility

It is the Customer's responsibility to ensure that unauthorised persons do not gain access to or misuse the Service Provider's service.

The Service Provider urges Customers 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 Customers and the Service Provider cannot be held liable for the Customer being placed on any bulk mailing lists as a result.

Where the Customer has authorised a minor to use any of the Service Provider's services or access its websites, you accept that as the parent/legal guardian of that minor, you are 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, including t=but not limited to transactions entered into by the minor using such access.

The Service Provider cannot be held liable for any business dealings you have with any third parties on the Internet, including any vendors, or advertisers found on, or through the Service Provider's network. Further, the Service Provider assumes no responsibility whatsoever for any charges you or any user of your account incurs when making purchases or other transactions in this manner. Further, the responsibility for ensuring compliance with all applicable customs and exchange control laws in connection with any such transactions shall be the Customer's.

Notice and Take-down Procedures

The Service Provider confirms that it has a procedure in place for the notice and take-down of illegal material. In compliance with section 77 of the Electronic Communications and Transactions Act (No. 25 of 2002) the Service Provider's designated agent being ISPA for this process can be reached at +27 11 314 7751 or on email address: complaints@ispa.org.za and at website http://www.ispa.org.za/co.

Customers are also notified of the content and procedures of the ISPA Code of Conduct (http://www.ispa.org.za/code) which may be used against any Internet service provider who fails to comply with the code of conduct.

Complaints and procedures

It is the Customer's responsibility to familiarise himself or herself with the procedure set out below and report any cases of violation of this AUP to the Service Provider's designated complaints handling agent.

Please note that the Service Provider cannot handle complaints concerning networks or users that do not have service contracts with us or our affiliates, or are outside of our control.

In order for the Service Provider to thoroughly investigate the complaint and take appropriate action all complaints must be in writing, via fax or email and contain as much information as possible, including, but not limited to:

- The origin of abuse or offence, including the website, full mail headers, relevant logfile extracts etc;
- Any contact details for the source of the complaint;
- A brief explanation why the incident is considered to be an offence.

The Service Provider discourages anonymous complaints being made via this service, and urges complainants to supply their name and contact details to us. Such information will not be released, except where requires by law enforcement. Anonymous complaints will however be acted upon as long as sufficient detail as outlined above is supplied.

Action following breach of the AUP

Upon receipt of a complaint, or having become aware of an incident, the Service Provider may take any of the following steps:

- In the case of a network, inform the user's network administrator of the incident and request the network administrator or network owner to deal address the incident in terms of this ISPA Code of Conduct;
- In severe cases suspend access of the user's entire network until abuse can be prevented by appropriate means;
- In the case of individual users, warn the user; suspend the user's account and/or revoke or cancel the user's network access privileges completely;
- Assist other networks or website administrators in investigating credible suspicions of any activity listed in this AUP;
- Institute a civil or criminal proceedings;
- Share information concerning the incident with other Internet access providers, or publish the information, and/or make available the user's details to the law enforcement agencies.

Reservation and Non Waiver of Rights

The Service Provider reserves the right to amend or alter this policy at any time.

The Service Provider reserves the right to take action against any individuals, companies or organizations that violate any of the prohibited activities set out herein, or engage in any illegal or unlawful activity while accessing our services, to the fullest extent of the law.

The Service Provider reserves the right, as 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 our network.

The Service Provider reserves the right to monitor user and network traffic for site security purposes and prevent any unauthorised attempts to tamper with our site or cause damage to our property.

The Service Provider reserves the right to suspend, revoke or cancel the Service Provider's services to the Customer/user if the safety and integrity of the Service Provider resources are placed at risk in continuing to provide service to the subscriber/user.

The Service Provider reserves the right to remove any information or materials in whole or in part, that, in the Service Provider's sole discretion, is deemed to be offensive, indecent, or otherwise objectionable.

The Service Provider does not undertake to guarantee the security of any data passing through its networks. Although the Service Provider will provide a "best effort" service, including regular updates on computer viruses and other threats to security of data, it is the responsibility of the communicating parties to safeguard their data, and the Service Provider cannot be held liable for any loss or damage arising as a result of the failure to do so.

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

Please send reports of any activity in violation of this Policy to: abuse@eoh-ns.co.za