THIS ACCEPTABLE USE POLICY ("AUP") IS A MATERIAL PART OF YOUR AGREEMENT WITH IUNCAPPED FOR PROVISION OF ITS SERVICES TO ITS CUSTOMERS. PLEASE READ AND FOLLOW THIS AUP CAREFULLY. THIS AUP MAY BE REVISED FROM TIME TO TIME BY IUNCAPPED.

This AUP forms part of the agreement between you and iUncapped and is incorporated by reference into iUncapped's terms and conditions. You and anyone who uses or accesses your iUncapped Internet services must comply with, and shall be bound by the terms of, this AUP.

1. LAWS AND REGULATIONS

Using iUncapped's service to transmit, distribute or store of any material in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secrets or other intellectual property right used without proper authorisation, and material that is, defamatory, constitutes hate speech , is an illegal threat, elicits violence or violates export control laws.

2. THE NETWORK

2.1. You acknowledge that iUncapped is unable to exercise control over the content of the information passing over its network and the Internet, including any websites, electronic mail transmissions, news groups or other material created or accessible over its network and/or services. Therefore, iUncapped is not responsible for the content of any messages or other information transmitted over its infrastructure.

2.2. You may obtain and download any materials marked as available for download off the Internet but are not permitted to use your Internet access to distribute any copyrighted materials unless permission for such distribution is granted to you by the owner of the materials.

2.3. You are prohibited from obtaining and/or disseminating any unlawful materials, including but not limited to stolen intellectual property, child sexual abuse material, hate-speech or materials that is intended to incite violence.

3. SYSTEM AND NETWORK SECURITY

3.1. All references to systems and networks under this section includes the Internet (and all those systems and/or networks to which user is granted access through iUncapped) and includes but is not limited to the infrastructure of iUncapped itself.

3.2. You may not circumvent user authentication or security of any host, network, or account (referred to as "cracking" or "hacking"), nor interfere with service to any user, host, or network (referred to as "denial of service attacks").

3.3. Violations of system or network security by you are prohibited, and may result in civil or criminal liability. iUncapped may investigate incidents involving such violations and will co-operate with law enforcement officials if a criminal violation is suspected. Examples of system or network security violations include, without limitation, the following:

3.3.1. Unauthorised access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of any system or network or to breach security or authentication measures without the express authorisation of iUncapped;

3.3.2. Unauthorised monitoring of data or traffic on the network or systems without express authorisation of iUncapped;

3.3.3. Interference with service to any user, host or network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks; and

3.3.4. Forging of any TCP-IP packet header (spoofing) or any part of the header information in an email or a newsgroup posting.

4. EMAIL USE

4.1. It is explicitly prohibited to:

4.1.1. send unsolicited bulk mail messages ("junk mail" or "spam") of any kind (commercial advertising, political tracts, announcements, etc.). This is strongly objected to by most Internet users and the repercussions against the offending party and iUncapped can often result in disruption of service to other users connected to iUncapped;

4.1.2. forward or propagate chain letters or malicious e-mail;

4.1.3. send multiple unsolicited electronic mail messages or "mail-bombing" to one or more recipient;

4.1.4. sending bulk electronic messages to recipients that have not opted in to receive such messages;

4.1.5. using redirect links in unsolicited commercial e-mail to advertise a website or service;

4.2. Your mail servers must be secured against public relay as a protection to both themselves and the Internet at large. 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. iUncapped 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 you. iUncapped also reserves the right to examine the mail servers of any users using iUncapped mail servers for "smarthosting". All relay checks will be done in strict accordance with iUncapped's policy of preserving customer privacy.

5. COMPLAINTS

5.1. Upon receipt of a complaint, or having become aware of an incident, iUncapped reserves the right to:

5.1.1. Inform you of the incident;

5.1.2. In the case of individual users suspend your account and withdraw your network access privileges completely.

5.1.3. In severe cases suspend your service until abuse can be prevented by appropriate means.

5.1.4. Share information concerning the incident with other Internet access providers, or publish the information, and/or make available users' details to law enforcement agencies.

5.2. All cases of violation of the above Acceptable Use Policy should be reported to iuncapped@iuncapped.co.za.