ACCEPTABLE USE POLICY

INTRODUCTION

This Acceptable Use Policy ('AUP') specifies the actions prohibited by users of Connect's network and systems and is intended to enhance the use of the Internet by preventing unacceptable use. Connect users are required to adhere to all the policies specified in this AUP without exception.

LAWS AND REGULATIONS

Connect's infrastructure may be used only for lawful purposes. Users may not violate any applicable laws or regulations of South Africa within the territory of South Africa. Should the user reside outside of South Africa, the laws of the country in which the user resides shall apply.

Transmission, distribution or storage of any material on or through the infrastructure in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret or other intellectual property right used without proper authorization, and material that is obscene, defamatory, constitutes an illegal threat, or violates export control laws.

THE NETWORK

The user acknowledges that Connect is unable to exercise control over the content of the information passing over the infrastructure and the Internet, including any websites, electronic mail transmissions, news groups or other material created or accessible over its infrastructure. Therefore, Connect is not responsible for the content of any messages or other information transmitted over its infrastructure. Connect's infrastructure may be used to link into other networks worldwide and the user agrees to conform to the acceptable use policies of these networks. The user may obtain and download any materials marked as available for download off the Internet but is not permitted to use its Internet access to distribute any copyrighted materials unless permission for such distribution is granted to the user by the owner of the materials. The user is prohibited from obtaining and/or disseminating on-line any unlawful materials, including but not limited to stolen intellectual property, child pornography, and/or any unlawful hate - speech materials.

SYSTEM AND SECURITY

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 Connect) and includes but is not limited to the infrastructure of Connect itself. The user 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"). Violations of system or network security by the user are prohibited, and may result in civil or criminal liability. Connect will investigate incidents involving such violations and will involve 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: Unauthorized 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 authorization of Connect

- Unauthorized monitoring of data or traffic on the network or systems without express authorization of Connect
- Interference with service to any user, host or network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks.
- Forging of any TCP- IP packet header (spoofing) or any part of the header information in an email or a newsgroup posting.

E-MAIL USE

It is explicitly prohibited to send unsolicited bulk e-mail messages ("junk mail" or "spam") of any kind (commercial advertising, political tracts, announcements, etc.). This is strongly objected by most Internet users and the repercussions against the offending party and Connect can often result in disruption of service to other users connected to Connect. Maintaining of mailing lists by users of Connect is accepted only with the permission and approval of the list members, and at the members' sole discretion. Should mailing lists contain invalid or undeliverable addresses or addresses of unwilling recipients those addresses must be promptly removed.
Users may not forward or propagate chain letters nor malicious e-mail. Public relay occurs when a mail server is accessed by a third party from another domain and utilized to deliver mails, without the authority or consent of the owner of the mail-server. Users' mail servers must be secure 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.
Connect 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. Connect also reserves the right to examine the mail servers of any users using Connect mail servers for "smart hosting" (when the user relays its mail off of a Connect 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 Connect's policy of preserving customer privacy.

NEWSGROUPS

Users should, before using the service, familiarize themselves with the contents of the following newsgroups: news, newusers.questions, news.announce. newusers, news.answers.
Excessive cross-posting (i.e., posting the same article to a large numbers of newsgroups) is forbidden.
Posting of irrelevant (off-topic) material to newsgroups (also known as USENET spam) is forbidden.
Posting binaries to a non-binary newsgroup is forbidden. Connect reserves the right to delete and/or cancel posts which violate the above conditions.

COMPLAINTS

Upon receipt of a complaint, or having become aware of an incident, Connect reserves the right to:
Inform the user's network administrator of the incident and require the network administrator or network owner to deal with the incident according to this AUP.
In the case of individual users suspend the user's account and withdraw the user's network access privileges completely. Charge the offending parties for administrative costs as well as for machine and human time lost due to the incident.

In severe cases suspend access of the user's entire network until abuse can be prevented by appropriate means.
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.

Any one or more of the steps listed above, insofar as they are deemed necessary by Connect in its absolute and sole discretion, may be taken by Connect against the offending party.

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