ACCEPTABLE USE POLICY (AUP)

1. INTRODUCTION

1.1 The purpose of this document is to provide an understanding of Service Provider's AUP. This policy serves to define the accepted behaviour of users on Service Provider's network. This allows Service Provider to:

1.1.1 maintain the integrity and quality of their services,

1.1.2 protect their customers and infrastructure from abuse,

1.1.3 adhere to the current laws and regulations governing organisations and service providers in the countries that they operate in,

1.1.4 co-exist within the global internet community as a responsible service provider.

2 THE NETWORK

1.1 The Customer acknowledges that Service Provider is unable to exercise control over the data passing over the infrastructure and the Internet, including but not limited to any websites, electronic mail transmissions, news groups or other material created or accessible over its infrastructure. Therefore, Service Provider is not responsible for data transmitted over its infrastructure.

1.2 Service Provider infrastructure may be used to link into other networks worldwide and the user agrees to conform to the acceptable use policies of these networks.

1.3 Users of the Service Provider network include not only the Service Provider customers, but in the case of resellers of the Service Provider's services, the customers of the resellers too. Resellers of Service Provider's services are responsible for the activities of their customers.

1.4 The user may obtain and download any materials marked as available for download off the Internet, but is not permitted to use their Internet access to distribute any copyrighted materials unless permission for such distribution is granted to the user by the owner of the materials.

1.5 The user is prohibited from obtaining, disseminating or facilitating over Service Provider's network any unlawful materials, including but not limited to

1.5.1 copying or dealing in intellectual property without authorization,

1.5.2 child pornography, and/or

1.5.3 any unlawful hate-speech materials.

1.6 To help ensure that all customers have fair and equal use of the service and to protect the integrity of the network, Service Provider reserves the right, and will take necessary steps, to prevent improper or excessive usage thereof.

1.7 The action that Service Provider may take includes, but is not limited to:

1.7.1 limiting throughput;

1.7.2 preventing or limiting service through specific ports or communication protocols; and/or

1.7.3 complete termination of service to customers who grossly abuse the network through improper or excessive usage.

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

1.9 Online activity will be subject to the available bandwidth, data storage and other limitations of the service provided, which Service Provider may, from time to time, revise at its own discretion and without prior notice to the Customer.

2. SYSTEM AND NETWORK SECURITY

2.1 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 Service Provider and includes but is not limited to the infrastructure of Service Provider itself.

2.2 The user may not circumvent user authentication or security of any host, device, network, or account (referred to as "cracking" or "hacking"), nor interfere with service to any user, host, device, or network (referred to as "denial of service attacks"). The host, device, network or account shall also not be used for any illegal purpose, including phishing.

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

2.4 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 Service Provider.

2.5 Unauthorised monitoring of data or traffic on the network or systems without express authorisation of Service Provider.

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

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

3. E-MAIL USE

3.1 It is explicitly prohibited to 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 Service Provider can often result in disruption of service to other users connected to Service Provider. In addition, Service Provider is entitled to take appropriate steps against the User in contravention of this provision.

3.2 Maintaining of mailing lists by users of Service Provider 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.

3.3 Users may neither forward nor propagate chain letters nor malicious e-mail.

3.4 Public relay occurs when a mail server is accessed by a third party and utilised 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.

3.5 Service Provider reserves the right to examine users' mail servers to confirm that their server is not a public relay and the results of such checks can be made available to the user. Service Provider also reserves the right to examine the mail servers of any users using Service Provider mail servers for "smart hosting", content filtering 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 Service Provider's policy of preserving customer privacy.

4. USENET NEWS

4.1 Users should, before using the service, familiarise themselves with the contents of the following newsgroups: news users' questions, news announcers, news users' answers.

4.2 Excessive cross-posting (i.e., posting the same article to a large numbers of newsgroups) is forbidden.

4.3 Posting of irrelevant (off-topic) material to newsgroups (also known as USENET spam) is forbidden.

4.4 Posting binaries to a non-binary newsgroup is forbidden.

4.5 Service Provider reserves the right to delete and/or cancel posts which violate the above conditions.

5. MANAGING ABUSE

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

5.2 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.

5.3 In the case of individual users suspend the user's account and withdraw the user's network access privileges completely.

5.4 Charge the offending parties for administrative costs as well as for machine and human time lost due to the incident.

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

5.6 Take such action as may be necessary to protect the integrity of the system, including, but not being limited to, system monitoring, as well as protocol management and shutting down of ports affected by viruses, worms or other malicious code.

5.7 Implement appropriate technical mechanisms in order to prevent usage patterns that violate this AUP.

5.8 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.

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

6. LAWS AND LEGISLATION

6.1 Service Provider's infrastructure may be used only for lawful purposes. Users may not violate any applicable laws or regulations of Kenya.

6.2 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 authorisation, and material that is obscene, defamatory, constitutes an illegal threat, or violates export control laws.

6.3 The User undertakes to use Service Provider's services in accordance with any restrictions imposed under the Kenya Information and Communication Act and any other legislation in Kenya.

7. LEGAL RIGHTS

7.1 Nothing contained in this policy shall be construed to limit Service Provider's rights or remedies in any way with respect to any of the aforementioned activities, and Service Provider reserves the right to take any action that it may deem appropriate with respect to such activities, including without limitation:

7.1.1 investigating suspected violations of this AUP,

7.1.2 taking action to recover costs and expenses incurred in identifying and resolving abuse,

7.1.3 terminating users' access to and use of the Dimension Data service;

7.1.4 levying cancellation charges to cover Service Provider's costs in the event of termination of the Dimension Data service.

7.2 In addition, Service Provider reserves all available rights and remedies with respect to such activities at law or in equity.

7.3 This AUP may be clarified or modified periodically and Service Provider reserves the right to modify this policy at any time, any such changes coming into effect as soon as they are published on Service Provider's parent company's website i.e. the Dimension Data website (www.dimensiondata.com).

7.4 This policy forms part of Service Provider's standard terms and conditions of service.

All cases of violation of the above AUP should be reported to: abuse.ke@dimensiondata.com and all cases of online child abuse and threats should be reported to: cop.ke@dimensiondata.com Reported cases will be forwarded to the relevant authorities for further investigations or reported directly to the Kenya Computer Incident Response Team Cordination Centre (KE-CIRT/CC) through the following contacts: incidents@ke-cirt.go.ke