FIBREHOOD ACCEPTABLE FAIR USE & ACCESS POLICY

1. PURPOSE

1.1 This policy serves to define the accepted behaviour of users on FIBREHOOD'S network.

1.2 The policy is intended to allow FIBREHOOD to:

1.2.1 maintain the integrity and quality of its service;

1.2.2 protect its Customers and infrastructure from abuse;

1.2.3 adhere to current laws and regulations governing organisations and service providers in Zimbabwe;

1.2.4 co-exist with the global internet community as a responsible service provider.

2. THE NETWORK

2.1 The Customer acknowledges that FIBREHOOD 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, FIBREHOOD is not responsible for data transmitted over its infrastructure.

2.2 The FIBREHOOD infrastructure may be used to link into other networks worldwide and the Customer agrees to abide by the acceptable use policies of these networks.

2.3 The Customer is prohibited from obtaining, disseminating or facilitating any unlawful materials over the FIBREHOOD network including, but not limited to:

2.3.1 copying or dealing in intellectual property without authorisation;

2.3.2 child pornography;

2.3.3 any unlawful hate-speech materials; and/ or

2.3.4 facilitation or funding of terrorist activities.

2.4 In order to ensure that all Customers have fair and equal use of the Service and to protect the integrity of the network, FIBREHOOD reserves the right, and will take whatever steps deemed necessary, to prevent improper or excessive usage of the Service. These steps may include but are not limited to:

2.4.1 any action required to prevent prohibited usage (whether intended or unintended) i.e. actions to prevent the spread of viruses, worms, malicious code, etc;

2.4.2 limiting throughput;

2.4.3 preventing or limiting services through specific ports or communication protocols;

2.4.4 complete termination of service to Customers who grossly abuse the network through improper or excessive usage;

2.4.5 suspending the Customer's account;

2.4.6 charge the offending Customer for administrative costs incurred as well as for machine and human time lost due to the incident;

2.4.7 implement appropriate mechanisms in order to prevent usage patterns that violate this policy; and/or

2.4.8 share information concerning the incident with other Internet access providers or publish the information and/or make available the Customer's details to law enforcement agencies.

3. SYSTEM AND NETWORK SECURITY

3.1 Any reference to systems and networks under this section refer to all systems and networks to which the Customer is granted access through FIBREHOOD, including, but not limited to, the infrastructure of FIBREHOOD itself and the Internet.

3.2 The Customer may not circumvent user authentication or security of any host, device, network or account (referred to as "hacking" or "cracking"), 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.

3.3 Violations of system or network security by the Customer are prohibited and may result in civil or criminal liability. FIBREHOOD will investigate incidents involving any violation or suspected violation and shall 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:

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 any security or authentication measures without the express authorisation of FIBREHOOD;

3.3.2 unauthorised monitoring of data or traffic on the network or systems without the express authorisation of FIBREHOOD;

3.3.3 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; and

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

4. INTERCEPTION

The Customer acknowledges that the FIBREHOOD network may be subject to laws relating to interception of communications and compliance shall be strictly in accordance with the provisions of the said Act.

5. GENERAL

5.1 This policy forms part of FIBREHOOD'S standard terms and conditions in respect of any of Fibrehood's Services and the usage of any FIBREHOOD Service shall be subject to this 'Annexure 2'.

5.2 Any cases pertaining to violation of this Acceptable Fair Use and Access Policy, must be reported to admin@fibrehood.co.zw.