This document (the "AUP") sets out the policies and guidelines applied by FiberRing in its relationship with Customer, in particular to clarify the manner in which the Services may be used by Customer and what manner of use is considered unacceptable by FiberRing. FiberRing's general terms and conditions (the "General Conditions"), and FiberRing's service schedules (the "Service Schedules"), are also part of the Agreement and apply to the Services provided by FiberRing.

1. DEFINITIONS

1.1. In addition to the definitions set out in the General Conditions and the Services Schedules, the following definitions shall apply:

Blacklist means a so called blacklist or block list which is a basic access control system that denies entry or access to a specific list or range of users or network addresses or IP addresses, as a result of which e-mail sent by a user or from a network address or from an IP address that is on the blacklist will not reach its intended destination or recipient.

DoS means Denial-of-Service.

End User means any client of Customer or other user of Customer's services, as well as any other person or (legal) entity who obtains access to Services via Customer.

IRC means Internet relay chat which is a form of real-time Internet text messaging or synchronous conferencing.

Mail Bomb means (i) e-mailing copies of a single message to many receivers; and/or (ii) sending large or multiple files or messages to a single receiver with malicious intent.

Spam means unsolicited bulk messages.

World Wide Web means a system of interlinked documents that runs over the Internet.

2. GENERAL

2.1. FiberRing aims to promote a high level of responsible behaviour in connection with the use of its Services, as well as, amongst others, the use of the Internet and the use of E-mail. For this purpose, FiberRing has created the AUP.

2.2. Customer must comply with the AUP and Customer is required to ensure that its End Users are aware of and comply with the AUP, as though such End User were a Customer. A breach of the AUP by an End User will also be considered a breach of the AUP by Customer.

3. CONTACT PERSONS

3.1. Customer shall designate (i) a contact person whom FiberRing may contact at any time in connection with (suspected) violations by Customer or its End Users of the AUP, (ii) a contact person whom FiberRing may contact at any time in the event of an emergency.

3.2. Customer will provide to FiberRing a means of contacting said contact person(s) at any and all times, and Customer shall ensure that the information set out in the FiberRing customer portal with respect these contact persons is and remains up to date.

4. USE OF SERVICES

4.1. Customer shall –and shall ensure that its End Users- only use the Services for lawful purposes and shall refrain from any use that breaches the AUP, the General Conditions, the Services Schedule, the Agreement or any applicable law.

4.2. Customer shall refrain from any use of the Services which may have an adverse effect on FiberRing's good name or standing, or may cause damage to FiberRing's business operations, or may subject FiberRing to litigation.

4.3. Specific activities that are prohibited include, but are not limited to: (i) terrorism; (ii) threatening harm to persons or property or otherwise harassing behaviour; (iii) compromising the security (or tampering with) system resources or accounts of other customers or of any other Internet sites or intranet sites without the proper authorisation; (iv) violating local export control laws for software or technical information; (v) the use or transmission or distribution of any data or material protected by IPRs without proper authorisation; (vi) the manufacture or use or distribution of counterfeit, pirated or illegal software or other product; (vii) providing or offering compensation to End Users based on download volume, unless Customer knows – or has no reason to doubt – that such End Users are using Customer's services only for lawful purposes and for the distribution or dissemination of their own data or material, or of data or materials for which they have the proper authorisation to distribute or disseminate the same; (viii) fraudulently representing products or services; (ix) Spamming, phishing, any DoS attacks without proper authorisation; (x) defamation; (xi) child pornography, child erotica and zoophilia ; (xii) activities that may result in the placement or inclusion on a Blacklist of Customer, Customer's IP address(es) and/or IP address(es) assigned by FiberRing to Customer; (xiii) intentionally accessing a computer system or infrastructure component without authorization or exceeding authorized access levels thereof; and (xiv) facilitating, aiding, or encouraging any of the foregoing activities.

5. ELECTRONIC MESSAGES / ANTI-SPAM

5.1. Customer may not (i) send electronic messages that in any way is or may be in breach of applicable law; (ii) send or propagate Spam and shall not allow its End Users or third parties to send or propagate Spam via Customer's IP addresses; (iii) send, propagate, or reply to Mail Bombs and shall not allow its End Users or third parties to send or propagate Mail Bombs via Customer's IP addresses; or (iv) alter the headers of electronic messages to conceal Customer's address or to prevent receivers from responding to messages.

5.2. Customer shall refrain from any activities that may result in the placement of Customer or Customer's IP address(es) on a Blacklist. FiberRing reserves the right to charge Customer three hundred Euros (€ 300.--) per hour in consulting fees for any remedial actions that FiberRing elects to take in the event that, as a result of Customer's activities, FiberRing's servers or IP address(es) are placed in any third-party filtering software or Blacklist.

5.3. Bulk messages are only permitted if (i) the Customer has obtained the explicit consent from each of the recipients via double opt-in, and/or (ii) applicable law permits the sending of such messages without the recipients' consent. Customer is obliged to offer in each electronic message, an easily accessible functioning unsubscribe mechanism, and Customer shall immediately cease sending electronic messages to a recipient after the recipient has unsubscribed.

6. WORLD WIDE WEB USE

6.1. Customer is prohibited from posting or transmitting illegal material on or via the Internet or the World Wide Web.

6.2. FiberRing is entitled to actively block ports or IP addresses for the Network, in the event that such is – in FiberRing's reasonable view – necessary to preserve or protect the security and performance of the Network or the Internet or the World Wide Web. An overview of the blocked ports or IP addresses may be requested in writing by Customer from FiberRing.

6.3. Without prejudice to the generality of Clause 6.2 of the AUP, FiberRing shall in any event actively block the following ports for its Network: (i) UDP/1434 - SQL slammer/worm; (ii) UDP/137 – Netbios; (iii) UDP/139 – Netbios; (iv) TCP/135 till 139 – Netbios; (v) TCP/445 – Smb; (vi) TCP/593 - Rpc endpoint mapper; and (vii) TCP/4444 - Blaster/worm.

6.4. If FiberRing reasonably suspects that Customer is subject to a DoS attack or another attack that results in an unaccounted peak in data traffic, FiberRing shall be entitled to immediately take measures to protect its infrastructure. In the event that Customer is subject to repetitive attacks, and Customer does not successfully take measures to prevent that future attacks may interfere with services provided by FiberRing to other customers or the use or operation of any Equipment, then FiberRing shall be entitled to immediately terminate the Agreement by sending a written notice to Customer.

7. IRC USE

7.1. Customer is prohibited from posting or transmitting inappropriate material via the use of IRC or to otherwise use IRC in a manner that is in breach of the AUP. For the purpose of this clause, prohibited use of IRC include so called 'eggdrops' and 'psybnc shell hosting'.

7.2. Without the prior written consent of FiberRing, which FiberRing may grant or deny in its sole and absolute discretion, Customer is prohibited from hosting an IRC server, regardless whether it concerns a stand-alone IRC server or an IRC server that connects to global IRC networks.

8. USE AND REGISTRATION OF IP ADDRESSES/AS NUMBERS

8.1. Customer shall comply with the policies, guidelines, terms and conditions applied from time to time by the organisation or entity which is responsible for the management (registration and/or distribution and/or giving into use) of IP addresses and AS numbers, i.e. the regional Internet registries of RIPE.

9. ABUSE HANDLING

9.1. In connection with use of Services, Customer shall adopt and apply an abuse handling procedure which is compliant with the AUP, with the law that applies to the Agreement and with any other law applicable to Customer.

9.2. If FiberRing is notified by a third party (including any law enforcement authority) of a (suspected) violation by Customer and/or the End User of the AUP and/or any applicable law, FiberRing shall notify Customer hereof by way of email or such other method of communication as FiberRing deems appropriate. Customer shall, within the response period or remedy period set forth in FiberRing's notification, take remedial action to cure the violation and within said remedy period inform FiberRing of the actions taken by Customer.

9.3. As a condition to the (continued) provision of Services and/or to resuming the provision of Services, FiberRing shall be entitled to require Customer: (i) to execute a cease and desist declaration; and/or - as appropriate - (ii) to confirm in writing that Customer's End User who was responsible for the violation, has been permanently excluded from using the Service.

9.4. Customer shall log (date and timestamp) each abuse notification received by Customer from FiberRing and from third parties, including the nature of the notification (e.g. copyright infringement), as well as Customer's response to such complaint, and the moment that Customer deems the abuse notification to be resolved. Customer shall maintain the log in respect of each abuse notification for a minimum of two (2) years after the date that Customer deems such abuse notification to be resolved.

9.5. Customer shall ensure the availability of sufficient and properly trained personnel to ensure that Customer's End Users comply with the AUP and to apply Customer's abuse handling procedure and to handle the volume of abuse notifications that arrive without backlogs.

9.6. If FiberRing is notified by a third party, including any law enforcement authority, of a (suspected) violation by Customer of any of the AUP, FiberRing shall be entitled to release any contact information with respect to Customer to such party.

9.7. Without prejudice to the above or any other provision of the FiberRing Policies, FiberRing does not intend to review, monitor or control as a precautionary measure all content sent or received by Customer using the Services. Accordingly, FiberRing accepts no responsibility or liability to Customer, or any other person for the content of any communications that are transmitted by or made available to Customer or its End Users, regardless of whether they originated from the Network or the Services.