This document 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 Sales Terms and Conditions and the Service Specifications and Support and Service Levels are also part of the Sales Contract and apply to the Services provided by FiberRing.

CHAPTER A. INTRODUCTION

1. DEFINITIONS

1.1. In addition to the definitions set out in the Sales Terms and Conditions, the Support and Service Levels and the Services Specifications, the following definitions shall apply:

Anonymous Proxy means a tool or instrument that accesses the Internet on a user's behalf via a proxy server.

Anonymous Proxy Provider means a business or organization that provides or makes available anonymous proxies as a service.

Authentification Details mean the logins, user identities, passwords, security questions, keys, tokens, URLs and other details that may be used to access the Service.

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.

DDoS means Distributed-Denial-of-Service.

DNS means domain name system, which is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network.

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.

Infrastructure means the Equipment, Service and Instances that support the flow and processing of information, including storage, servers and networking components.

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.

Malicious Software means any type or form of malicious or hostile Software, including but not limited to computer viruses, worms, trojan horses, and spyware (*malware*).

PTR Record means a pointer record, which is a type of DNS record that resolves an IP address to a domain or host name.

Spam means unsolicited bulk messages.

TOR means the onion router, which is software for enabling anonymous communication that routes traffic through multiple anonymizing nodes**.**

TOR Exit Node means the final node that Tor traffic is routed through before it reaches its final destination.

VPN means virtual private network, which is a service that extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

VPN Provider means a business or organization that provides VPN services.

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 these Policies.

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

2.3 FiberRing is entitled to issue new versions and thereby amend the Policies. Such amendment applies to existing and new Contracts for Services, unless FiberRing states otherwise formally in writing. The amendments come into effect immediately after made available on FiberRing's website.

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 Policies, (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. AUTHENICATION DETAILS

4.1. Some Services may only be accessible through the use of Authentication Details. Customer is solely responsible for the maintenance, security and use of its Authentication Details. All consequences and losses relating to the use of Customer's Authentication Details, whether or not Customer has authorized that use, shall be for Customer's sole account, including all business and communication conducted with FiberRing through the use of its Authentication Details.

4.2. To the extent possible, Customer shall change its Authentication Details immediately upon receipt thereof by Customer, and Customer shall change the Authentication Details regularly thereafter. Customer will ensure that it will employ best practices when generating Authentication Details.

4.3. If Customer knows or suspects that the security of its Authentication Details has been compromissed, or that its Authentication Details are misused, Customer must, as soon as possible, notify FiberRing and immediately change its Authentication Details.

CHAPTER B. ACCEPTABLE USE POLICY

5. USE OF SERVICES

5.1 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 Sales Contract including these Policies or any applicable law.

5.2 Without prejudice to the law that applies to the Sales Contract, the Customer acknowledges and agrees that the Customer's use –and its End User's use- of the Services is to be compliant with (mandatory) law of the Netherlands, as well as with other laws applicable to Customers or its use of the Service.

5.3 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.

5.4 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 Intellectual Property Rights 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, DoS attacks, DDoS attacks, DRDoS attacks without proper authorisation; (x) defamation; (xi) zoophilia, (xii) child pornography, and virtual child pornography, and child erotica and zoophilia ; (xiii) intentionally accessing a computer system or Infrastructure structure component without authorization or exceeding authorized access levels thereof; (xiv) 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; (xv) non-authorized scans and/or penetration testing; and (xvi) facilitating, aiding, or encouraging any of the foregoing activities.

6. ELECTRONIC MESSAGES / ANTI-SPAM

6.1 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.

6.2 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 the Express Delisting Fees as stipulated on the UCEProtect website for Level 2 Listing of a FiberRing's IP range(s) and/or Level 3 Listing of FiberRing's ASN or 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 or Customer's end-user(s), FiberRing's servers or IP address(es) are placed in any third-party filtering software or Blacklist or the FiberRing's IP range(s) and/or ASN are placed on the UCEProtect Blacklist.

6.3 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.

7. INTERNET USE

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

7.2. 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.

7.3 Without prejudice to the generality of Clause 7.2 of the Acceptable Use Policy, 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; (vii) TCP/4444 - Blaster/worm; and (viii) Protocol UDP port 11211 – Memcache.

7.4 If FiberRing reasonably suspects that Customer is subject to a DoS attack DDoS attack, DRDoS attack or another attack and (in FiberRing's opinion) such attack negatively affects the Infrastructure, 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 negatively affect FiberRing's infrastructure, then FiberRing shall be entitled to immediately terminate the Sales Contract by sending a written notice to Customer.

8. IRC USE

8.1 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 Acceptable Use Policy. For the purpose of this clause, prohibited use of IRC include so called 'eggdrops' and 'psybnc shell hosting'.

8.2 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.

9. USE OF THE CUSTOMER PORTAL

9.1. Subject to the terms of use applied from time to time by FiberRing, and subject to the provisions of the Sales Contract, and Customer's compliance therewith, FiberRing shall arrange that FiberRing will grant a non-exclusive, non-transferable, non-assignable, non-sublicensable and royalty free right to use the Customer Portal during the Term. Use of the Customer Portal by or on behalf of Customer shall be at Customer's risk and responsibility.

9.2. Customer shall observe each and any instruction of FiberRing regarding the use of the Customer Portal.

10. USE AND REGISTRATION OF (INTERNET) DOMAINS/ IP ADDRESSES/AS NUMBERS

10.1 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 an (Internet) domain, such as – for example – ICANN.

10.2 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.

CHAPTER C. ABUSE COMPLIANCE POLICY

11. ABUSE HANDLING REQUIREMENTS

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

11.2 Customer shall log (date and timestamp) each Abuse Notification (as defined below) 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.

11.3 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. Customer will provide FiberRing with a copy of its Abuse Notification log, upon FiberRing's request.

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

11.5 If a Customer is a VPN Provider or Anonymous Proxy Provider, Customer shall be obliged to comply with the following requirements in connection with the use of the Services:

a) Customer's company information must be visible and available on its website (including a publicly-available email address for abuse handling purposes and copyright-related complaints),

b) Customer shall enter into an user-agreement with its End Users that shall include provisions to ensure an End User's compliance with applicable law, including but not limited to intellectual property law, and with the Policies,

c) Customer shall maintain accurate rDNS/PTR records containing Customer identifying information for all IP addresses that are used by Customer and/or its End Users to to provide VPN / Anonymous Proxy services,

d) when requested by Leaseweb at Leaseweb's sole discretion, Customer shall provide the relevant information required for Leaseweb to update Leaseweb rWHOIS records with the correspondent regional IP address registry, within a reasonable time as indicated in the request,

e) Customer shall comply with the repeat infringer policy in Section 14,

f) Customer shall implement and apply reasonable measures to prevent an End User -that has been terminated for repeat-infringement- from recommencing the use of Customer's services or the use of the Services through or via Customer,

g) Customer shall implement and apply technical measures designed to inhibit non-compliant or infringing activities.

11.6 If a Customer is a Tor-Exit node Operator, Customer shall be obliged to comply with the following requirements in connection with the use of the Services: (i) Customer shall in any event actively close/block such ports that are generally known to be used or are generally associated with non-compliant or infringing activities, a list of which may from time to time be published by Leaseweb or provided to Customers, (ii) Customer's rDNS records shall start with 'tor.exit.node.', (iii) Customer shall add a working email address to the 'torrc' file to allow for direct contact with Customer if required by End Users or third parties.

11.7 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.

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.

12. ABUSE PROCEDURE

12.1. 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 Acceptable Use Policy and/or any applicable law (an "**Abuse Notification**"), FiberRing shall notify Customer hereof by way of email or such other method of communication as FiberRing deems appropriate.

12.2. Customer shall, within the response period or remedy period set forth in FiberRing's notification (the "**Remedy Period**"), take remedial action to cure the violation and within the Remedy Period inform FiberRing of the actions taken by Customer.

12.3. In some cases, FiberRing may grant the Customer the option to contest the alleged violation by filing a counter notice (a "**Counter Notice**"). If Customer chooses to file a Counter Notice, Customer must use the online form made available to Customer for this purpose. FiberRing shall review the submitted information and may (in FiberRing's sole discretion) decide to reject Customer's Counter Notice, and require Customer to take immediate remedial action, if – in FiberRing's sole discretion – Customer's or the End-User's content or actions are unmistakably unlawful and/or may subject FiberRing to third party claims and/or litigation.

12.4. If FiberRing does not reject Customer's Counter Notice, Customer shall - upon FiberRing's request - provide a deposit or a bank guarantee or a parent guarantee or other security satisfactory to FiberRing. The amount of the security will be determined by FiberRing at its sole discretion. The security is intended to cover Customer's obligations, and any claim of FiberRing, under the indemnity specified in the Sales Terms and Conditions. Furthermore, in the event that Customer files a Counter Notice, Customer shall within two (2) days of its response to FiberRing notify FiberRing whether an attorney will be representing Customer and, if so, which attorney.

12.5. Customer shall provide FiberRing with all documents and information in connection with the Abuse Notification without cost and on first demand.

12.6. 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.

13. REPEAT INFRINGERS AND LIVE VIDEO STREAMS

13.1. As part of its abuse handling procedure, Customer should make reasonable efforts to detect repeated attempts by its End Users to store, transfer, or distribute - on or through Customer's services - (i) materials or data which violate or infringe the Acceptable Use Policies; or (ii) that Customer previously deleted or disabled following receipt of an Abuse Notification.

13.2. Customer shall immediately terminate the provision of service to an End User -and terminate an End User's access to the Services, in the event that such End User is discovered to be a repeat infringer or violator of the Leaseweb Policies.

13.3. Customer shall, upon request, demonstrate compliance with the following requirements:

a) Confirm it has established and implemented its own repeat infringer policy;
b) Publish a publicly available statement or policy prohibiting use of its services to infringe copyright;

13.4 Publicly designate a copyright abuse agent (including a publicly available email address);In the event Customer's services are repeatedly used for streaming of live video and/or audio, Customer shall offer an online take down tool to trusted third parties (or their agents) to allow them to immediately terminate live video streams which are infringing on the intellectual property rights of these trusted third parties.

CHAPTER D. FAIR USE POLICY

14 FAIR USAGE

14.1 The Service is provided for Customer's normal, fair, and reasonable use. In any event, Customer's use shall be deemed unfair and unreasonable, if Customer's Burst at any point in time exceeds three (3) times the Commitment.

14.2 In the event FiberRing, in its sole discretion, determines that the Customer is not using the Service according to this Fair Use Policy, FiberRing will, without any prior notice, be entitled to immediately impose limits on the speed of the data the Customer may transmit and/or receive with the Service.

15 IP CONNECTIVITY

15.1 The IP Connectivity Service is provided for Customer's consistent, fair, and reasonable use.

15.2 Customer's use of IP Connectivity shall be deemed unfair and unreasonable, if FiberRing determines (in its sole discretion) that Customer's actual or projected use of IP Connectivity exceeds, or is likely to exceed, the monthly Committed Bandwidth or Committed Data Traffic, and such use affects the provision of services by FiberRing to other FiberRing customers. If the Customer has not agreed to Committed Bandwidth or Committed Data Traffic, then for the purpose of interpreting this Clause 14.2 only, the Committed Bandwidth or Committed Data Traffic (as applicable) shall be deemed the lowest value of the Committed Bandwidth or Committed Data Traffic offered by FiberRing for the respective Service.

15.3 Customer's use of IP Connectivity is deemed to be inconsistent, if Customer's use thereof results in irregular Bandwidth or Data Traffic usage patterns, either on a per server basis or as part of a group of Customer's servers/Instances.

15.4 Storage components of the Cloud Platform are provided to Customer on a shared storage system, and therefore Customer's use of the Cloud Services may affect the performance (such as latency, storage bandwidth and IOPS) of the storage system as a whole. To protect the performance and integrity of the Cloud Platform, Customer shall ensure that its use of the storage shall be fair and reasonable.

CHAPTER E. SECURITY POLICY

16 INFRASTRUCTURE CONFIGURATION

16.1 FiberRing promotes a high level of responsible behavior in connection with the use of FiberRing services and requires that users of FiberRing Services do the same. For this reason, FiberRing has established information security requirements for all FiberRing Services, including standards for the basic configuration of Infrastructure, the use of Authentication Details and the use of effective Malicious Software detection and prevention.

16.2 Customer is advised (i) to back-up (critical) data and system configurations on a regular basis and store such data in a safe place, and (ii) not to connect its Infrastructure via a wireless connection, (iii) to keep the Software operated or used on the Infrastructure up to date, and accordingly to install updates and patches on a regular basis without undue delay after becoming available, (iv) to operate and/or use adequate measures against Malicious Software on the Infrastructure.

16.3 Customer shall ensure that all data distributed through the Service shall be free of Viruses. FiberRing may, without giving any notice and without incurring any liability vis-à-vis Customer, (temporarily) suspend or (temporarily) disconnect from the Network, any Service found to be infected with a Virus. The suspension shall continue until the Virus has been removed and the infection has been cured.

17 MONITORING / REPORTING

17.1 Customer shall implement logging and monitoring measures for security-related events.

17.2 Customer shall immediately report to FiberRing's NOC any security-related event that may materially impact FiberRing's Infrastructure, FiberRing's organisation or FiberRing's provision of services to other customers. Customer shall make the log in relation to such event immediately available to FiberRing upon FiberRing's request, and shall follow any directions given by FiberRing's as may be required to contain or correct the event.

CHAPTER F. INVESTIGATION AND ENFORCEMENT POLICY

18 INVESTIGATION

18.1 FiberRing reserves the right to conduct an investigation, based on (i) suspected violations of the Policies; and/or (ii) (potential) security risks to its Infrastructure; and/or (iii) a valid request of the relevant (law enforcement) authorities.

18.2 As part of this investigation, FiberRing may, acting reasonably (i) gather information from or about Customer; (ii) if relevant, gather information from a complaining party; and/or (iii) review and investigate Customer's security log referenced in Clause 17. Customer is obliged to fully cooperate with any such investigations by FiberRing.

19 FIBERRING ACTION

19.1 To the extent legally required, FiberRing is authorised to grant relevant law enforcement authorities access to Customer's content, information and/or Infrastructure, as well as any information gathered in the investigation conducted by FiberRing.

19.2 Upon request of a third party, FiberRing shall be entitled to disclose identifying Customer information to said party in connection with a (suspected) breach of the FiberRing Acceptable Use Policies to the extent required by law (such to be determined in FiberRing's discretion).

19.3 FiberRing shall be entitled to take action, legal or otherwise, against Customer and/or and End User, in the event that the use of the Service by Customer or its End User(s), breaches the Policies, or Customer allegedly fails to comply with any obligation under the Policies. The appropriate action will be determined by FiberRing, in its sole discretion, and may include: (a) suspension or termination of any or all of the Services in accordance with the Sales Terms and Conditions; (b) (selective) IP or port blocking; (c) reinstallation of the Services; (d) imposing limits on the use of Service (such as imposing limits on the speed of the data the Customer may transmit and/or receive with the Service); (e) restarting the Service, (f) blocking access at the router and/or switch level of Customer's Infrastructure; (g) denying Customer (physical) access to Infrastructure; (h) providing binding instructions to Customer in regards of the use of the Services, (i) changing or updating Customer PTR, rDNS or rWHOIS record;s and/or (j) placing files infected by Malicious Software in quarantine.

20 DISCLAIMER

20.1 Without prejudice to the above or any other provision of the Policies, FiberRing does not intend to review, monitor or control as a precautionary measure content sent or received by Customers using the Services. Accordingly, FiberRing is not responsible or liable 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.

20.2 None of the provisions of this Chapter F or any of the other Chapters of the Policies shall in any way limit or prejudice any other rights or remedies FiberRing may have.