This document sets out the Policies and guidelines applied by Leaseweb in its relationship with Customer, in particular to clarify the manner in which the Services and Equipment may be used by Customer and what manner of use is considered unacceptable by Leaseweb. Leaseweb's Sales Terms and Conditions, Services Specifications, and Service Level Agreement are also part of the Sales Contract and apply to the Services and any Equipment provided by Leaseweb.

CHAPTER A. INTRODUCTION

1. DEFINITIONS

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

Acceptable Use Policies means Chapter B of these Policies.

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 email 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.

CSEM means Child sexual exploitation material including child erotica material.**DDoS** means Distributed-Denial-of-Service.

Deep fakes means the use of an AI system to digitally manipulate (synthetic) audio or visual media capable of generating highly realistic videos or falsely appear to be an existing person.

Digital Services Coordinator means the Digital Services Coordinator as mentioned in the Regulation (EU) 2022/2065 of The European Parliament and Of The Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

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.

DRDoS means Distributed-Reflected-Denial-of-Service.

DSA means the Regulation (EU) 2022/2065 of The European Parliament and Of The Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

Offlimits means the foundation Offlimits (with the Chamber of Commerce number 41217108), incorporated under the laws of the Netherlands, an expertise bureau for combating and prevention of online abuse.

Hit means each individual time a file is sent to the End–User by the CDN Platform.

Hit Factor shall be a fraction, the numerator of which is the number of Hits that have occurred a month, and the denominator is the Utilized Data Traffic for that month measured in GB.

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

ICANN means Internet Corporation for Assigned Names and Numbers, a not-for-profit public-benefit corporation, which is among other responsible for managing the Internet Protocol address spaces and assignment of address blocks to regional Internet registries, for maintaining registries of Internet protocol identifiers, and for the management of the top-level domain name space.

Instant Image Identifier (I3) means a technical tool that transforms any image or video into a hash. This I3 tool allows Customers to check whether files uploaded to their databases are of known CSEM or images for punishable hashes.

IRC means Internet relay chat.

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*).

Member State means a member state of European Union.

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

Popular Cached Content means the part of Customer's content that is requested by End-Users in a 48 hourperiod and is cached on Leaseweb's CDN.

rDNS means reverse DNS, which determines the domain name associated with an IP address. It is used to identify the name of the service provider assigned to an IP address.

RIPE means Réseaux IP Européens, i.e. a collaborative forum open to all parties interested in wide area Internet Protocol networks and the (technical) development of the Internet.

SIDN means the foundation, incorporated under the laws of the Netherlands, for Internet Domain Registration in the Netherlands (Stichting Internet Domeinregistratie Nederland).

Spam means unsolicited bulk messages.

TCO means the terrorist content online as set forth in Regulation 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online.

TCO Regulation means the Regulation 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online.

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. Leaseweb 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 email. For this purpose, Leaseweb 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. Leaseweb is entitled to issue new versions and thereby amend the Policies. Such amendment applies to existing and new Contracts for Services, unless Leaseweb states otherwise formally in writing. The amendments come into effect immediately after made available on Leaseweb's website.
2.4. At all times, the Customer shall comply with Leaseweb's KYC requirements to be determined at its discretion in order to ensure Customer good standing of its business and/or related staff including export control compliance and sanctions as part of Leaseweb's Acceptable Use Policy requirements. In case Leaseweb has reasonable doubts of Customer good standing of its business and/or related staff and/or is subject to any export control restriction globally, whatever the source, Leaseweb is entitled to immediately suspend and terminate the Sales Contract and cease all Services, without incurring any liability for costs, expenses and damages as a result of the Customer's non-compliance with Leaseweb's Acceptable Use Policy including KYC check and/or the termination of the Sales Contract.

3. CONTACT PERSONS

3.1. Customer shall designate (i) contact persons whom Leaseweb may contact at any time in connection with (suspected) violations by Customer or its End Users of the Policies, (ii) contact persons whom Leaseweb may contact at any time in the event of an Emergency.
3.2. Customer will provide to Leaseweb a means of contacting said contact person(s) at any and all times, and Customer shall ensure that the information set out in the Customer Portal with respect these contact persons is and remains up to date.

4. AUTHENTICATION 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 Leaseweb 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 compromised, or that its Authentication Details are misused, Customer must, as soon as possible, notify Leaseweb and immediately change its Authentication Details.

CHAPTER B. ACCEPTABLE USE POLICY

5. USE OF SERVICES

5.1. Customers 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 Leaseweb 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 Leaseweb's good name or standing, or may cause damage to Leaseweb's business operations, or may subject Leaseweb to litigation.
5.4. Specific illegal content and illegal activities that are prohibited include, but are not limited to: (i) terrorism and/or dissemination to the public of terrorist content online TCO; (ii) threatening harm to persons or property or otherwise harassing behaviour; (iii) violating local export control laws for Software or technical information; (iv) the use or transmission, reproduction or distribution of any data or material that infringes any Intellectual Property Rights; (v) the manufacture or use or distribution of counterfeit, pirated or illegal software or other product; (vi) 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; (vii) fraudulently representing products or services; (viii) defamation, zoophilia, child pornography and virtual child pornography, and child erotica; (ix) illegal content and disinformation and illegal deep fakes; (xi) 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; (xii) Spamming, phishing, DoS attacks, DDoS attacks, DRDoS attacks without proper authorisation; 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 Leaseweb to Customer; (xv) non-authorized scans and/or penetration testing and (xvi) facilitating, aiding, or encouraging any of the foregoing activities (.

5.5. Customer acknowledges that any use by Customer and/or its End Users of the Services in breach of the Acceptable Use Policy could subject Customer and/or its End Users to criminal and/or civil liability, in addition to other actions by Leaseweb outlined in Chapter G of the Policies and in the Sales Terms and Conditions.

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. Leaseweb reserves the right to charge Customer the Express Delisting Fees as stipulated on the UCEProtect website for Level 2 Listing of a Leaseweb's IP range(s) and/or Level 3 Listing of Leaseweb's ASN or three hundred Euros (€ 300,--) per hour in consulting Fees for any remedial actions that Leaseweb elects to take in the event that, as a result of Customer's activities or Customer's end-user(s), Leaseweb's servers or IP address(es) are placed in any third-party filtering software or Blacklist or the Leaseweb'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. Leaseweb is entitled to actively block ports or IP addresses for the Network, in the event that such is – in Leaseweb'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 Leaseweb.

7.3. Without prejudice to the generality of Clause 7.2 of the Acceptable Use Policy, Leaseweb shall in any event actively block the following ports for its Network: (i) UDP/137 – Netbios; (ii) UDP/139 – Netbios; (iii) TCP/135 till 139 – Netbios;(iv) TCP/445 – Smb; and (v) Protocol UDP port 11211 – Memcache.

7.4. If Leaseweb reasonably suspects that Customer is subject to a DoS attack, DDoS attack, DRDoS attack or another attack and (in Leaseweb's reasonable opinion) such attack negatively affects the Infrastructure, Leaseweb shall be entitled to immediately block access to Customer's 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 Leaseweb's Infrastructure, then Leaseweb shall be entitled to immediately terminate theSales 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 Leaseweb, which Leaseweb 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 Leaseweb Global B.V., and subject to the provisions of the Sales Contract, and Customer's compliance therewith, Leaseweb shall arrange that Leaseweb Global B.V. 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 Leaseweb Global B.V. 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.

11. RESTRICTIONS ON USE OF SHARED WEB HOSTING SERVICES

11.1. Customer may not:

a) use the Shared Web Hosting Services in a manner that may interfere with or otherwise disrupt services to other customers of Leaseweb or Leaseweb's infrastructure or that may cause an Emergency;

b) knowingly allow any other website or hosting server to link to content stored on Leaseweb's systems. At least 75% of any content stored on Leaseweb's systems must have associated HTML, PHP or similar files at the Shared Web Hosting Service linking to the content stored on the Shared Web Hosting Services;

c) exceed the Shared Web Hosting Services limits, such as allotted diskspace or bandwidth;
d) run scheduled tasks, such as cron entries, with intervals of less than fifteen (15) minutes;
e) run stand-alone, unattached server side processes or deamons on the Shared Web Hosting Platform;
f) send more than 3 emails per minute/180 emails per hour; and/or
g) use Shared Web Hosting Services for hosting Mailer Pro, Push button mail scripts, proxy scripts/anonymizers, autoSurf/PTC/PTS/PPC sites, spiders, crawlers, indexers, banner-ad services (commercial banner ad rotation).

11.2. If Leaseweb detects failed login attempts to the Shared Web Hosting Service, it may, without notice and whithout obligations of any kind, ban network access from the source of those failed attempts.

CHAPTER C. ABUSE COMPLIANCE POLICY

12. ILLEGAL CONTENT AND ABUSE HANDLING

12.1. In connection with use of the 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, including the DSA.

12.2. Customer shall log (date and timestamp) each Abuse Notification (as defined below) received by Customer from Leaseweb 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.

12.3. 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 Leaseweb with a copy of its Abuse Notification log, upon Leaseweb's request.

12.4. 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.

12.5. In order to prevent any breach of Clause 5.4 of the Policies, the Customer shall fulfill its obligation on behalf of its End Users to demonstrate and timely execute its fully compliant proper performance of these Policies.

12.6. 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 a 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 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.

12.7. 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.

12.8. In connection with the use of the Services, Customer shall be obligated and is responsible for the pro-active initiatives for purposes of technical adoption, contractual engagement and active use of the Instant Image Identifier (I3) operated by Offlimits for any user generated content websites in order to fully prevent any abuse of illegal content and non-compliant use of the Service in breach of Clause 5.4 of the Fair Use Terms, thereby fulfulling Customer's obligation on behalf of its End Users to demonstrate its full compliance. In addition, if Customer is notified by the Compliance department to undertake this responsibility, Customer shall be obliged to report to Offlimits within twenty-four (24) hours to sign the agreement for acceptance and implementation of the Instant Image Identifier (I3) guaranteeing towards Offlimits and Leaseweb the active use thereof. This obligation is deemed a guaranteed performance by Customer also for and on behalf of its End Users for whom the Customer shall be held responsible and liable. The obligation by Customer for the Offlimits engagement and active use of the Instant Image Identifier (I3) is part of Leaseweb's continuous zero tolerance approach towards any CSEM content notified and/or found within its network. If Customers fails to comply with the Policies to prevent CSEM and Child erotica in accordance with this continued zero tolerance approach and/or fails to fully and adequately remove such content within the deadlines notified by Leaseweb, Leaseweb is entitled - for each of such failure or alleged circumstances to expect such failure - to disable and suspend the Services by means of null routing and terminate the Services.

12.9. Customer acknowledges that a failure to comply with Clause 12.8 by Customer and/or its End Users of the Services shall result in an immediate material breach of the Acceptable Use Policy without any requirement of Leaseweb's further notifications . Leaseweb is entitled at its full discretion to immediately suspend and/or terminate the Services and Sales Contract without Leaseweb incurring any liability for such termination or any damages and costs resulting thereof while the Customer shall keep Leaseweb fully indemnified for any damages including reputation and immaterial, indirect and consequential damages and will keep Leaseweb harmless for any third party claims.

12.10. In connection with the use of the Services, Customer shall be obligated and is responsible for the satisfactory pro-active initiatives on behalf of itself and its End Users to fully prevent dissemination of terrorist content online by making use of the Services.

a) In order to fully prevent any dissemination of TCO and breach of Clause 5.4 of the Leaseweb Policies, the Customer shall fulfill its obligation on behalf of its End Users to demonstrate and timely execute its fully compliant proper performance of these Policies, based on the TCO Regulation and instructions from a national competent authority.

b) If Customer is notified by the Leaseweb Compliance department and/or a national competent authority to undertake this Customer responsibility on behalf of itself and its End Users, Customer shall be obliged to timely remove reported prohibited content within one (1) hour, in accordance with the TCO. This obligation is deemed a Customer warranty for and on behalf of its End Users for whom the Customer shall be held responsible and liable to represent and undertake its compliance with the TCO and to indemnify and keep Leaseweb harmless.

c) If Customers fails to comply with the Policies and/or instructions from a national competent authority to prevent such prohibited content in accordance with the TCO Regulation and/or fails to fully and adequately remove such content within the deadlines notified by Leaseweb and set forth in the TCO Regulation, Leaseweb applies its zero tolerance approach, Leaseweb is entitled - for each of such failure or alleged circumstances to expect such failure - to disable and suspend the Services by means of null routing and terminate the Services.

13. ABUSE AND ILLEGAL CONTENT PROCEDURE

13.1. Leaseweb has an Abuse and illegal content Procedure ("**Abuse Procedure")** which is set out on https://www.leaseweb.com/abuse-handling. This gives third parties the option to notify ("**Notifier**") Leaseweb by e-mail of (alleged) illegal content and abusive material that is accessible via its Services.

13.2. If Leaseweb is notified by a Notifier (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**"), Leaseweb shall notify Customer hereof by way of email or such other method of communication as Leaseweb deems appropriate and in accordance with the DSA.

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

13.4. In some cases, Leaseweb 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. Leaseweb shall review the submitted information and may (in Leaseweb's sole discretion) decide to reject Customer's Counter Notice, and require Customer to take immediate remedial action, if – in Leaseweb's sole discretion – Customer's or the End-User's content or actions are unmistakably unlawful and/or may subject Leaseweb to third party claims and/or litigation.

13.5. If Leaseweb does not reject Customer's Counter Notice, Customer shall – upon Leaseweb's request – provide a deposit or a bank guarantee or a parent guarantee or other security satisfactory to Leaseweb. The amount of the security will be determined by Leaseweb at its sole discretion. The security is intended to cover Customer's obligations, and any claim of Leaseweb, 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 Leaseweb notify Leaseweb whether an attorney will be representing Customer and, if so, which attorney.

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

13.7. As a condition to the (continued) provision of Services and/or to resuming the provision of Services, Leaseweb 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.

13.8. If Customer does not respond (in a timely manner) to an Abuse Notification that Leaseweb has forwarded to the Customer, or if Customer does not take the necessary remedial measures (in a timely manner) or does not follow up a notification in a timely manner within the set deadline, Leaseweb shall take measures against the Customer in order to prevent further violations of applicable law and the Leaseweb Policies.

14. STATEMENT OF REASONS

14.1. If Leaseweb has taken an action that has restricted the Services in accordance with the DSA, it will provide a clear and specific statement of reasons to affected Customer of the Service for any of the following restrictions imposed on the ground that the information provided by the Customer of the Service is illegal content or incompatible with the Policies or applicable laws. This shall not apply where the information is deceptive high-volume commercial content (SPAM).

14.2. Leaseweb shall act in a diligent, objective, and proportionate manner in applying and enforcing the restrictions, with due regard to the rights and legitimate interests of all parties involved, including the fundamental rights of the Customer, such as the freedom of expression, freedom and pluralism of the media, and other fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights.

14.3. The statement of reasons shall be given no later than the date on which the restriction is imposed, irrespective of why or how it was imposed.

14.4. The statement of reasons shall contain at least the following information (i) the facts and circumstances on which the decision is based, including, where appropriate, whether the decision was taken as a result of a notification made under Article 16 DSA; (ii) if the decision is based on the alleged incompatibility of the information with Leaseweb's Sales Terms and Conditions and/or Policies, a reference to the relevant contractual provision and an explanation of why the information is considered incompatible with it.

14.5. If Customer objects to any measures Leaseweb has taken, whether it is after a notice, or following other information, Customer can send a detailed response (with all documents and information in connection with the Abuse Notification) with motivation to dsa@global.leaseweb.com within six months after the date Leaseweb has taken action, provided the Sales Contract has not been cancelled or terminated within this time frame. Leaseweb will then decide within a reasonable period whether the taken measures were justified, or that another action should be taken.

14.6. If the Customer is not satisfied with the results of the internal compliant-handling mechanism as stated in the previous clause, then Customer reserves the right to initiate legal proceedings against the statement of reasons with the before the competent court under applicable law.

15. REPEAT INFRINGERS AND LIVE VIDEO STREAMS

15.1. 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.

15.2. 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.

15.3. 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;

15.4. 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

16. IP CONNECTIVITY

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

16.2. Customer's use of IP Connectivity shall be deemed unfair and unreasonable, if Leaseweb 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 by more than 100%, and such use affects the provision of services by Leaseweb to other Leaseweb customers. If the Customer has not agreed to Committed Bandwidth or Committed Data Traffic, then for the purpose of interpreting this clause 15.2 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 Leaseweb for the respective Service.

16.3. 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.

16.4. Should Customer's Traffic pattern result in an ASN Destination Percentage for a certain ASN number higher than the percentages below (the "**ASN Threshold**"), then the Data Traffic or Bandwidth in excess of the ASN Threshold shall be charged at EUR 3,00 (three euro) per TB or EUR 0,75 (seventy-five euro-cents) per Mbps on top of the contracted rate.

Table 1: ASN Thresholds

ASN DESTINATION	REGION	ASN THRESHOLD
AS701 (Verizon)	US	10%
7922 (Comcast)	US	10%,
20115 (Charter)	US	10%
7018 (AT&T)	US	10%
AS9121 (Turktelecom)	EU	10%
AS3320 (DTAG)	EU	5%
AS3352 (Telefonica)	EU	10%
AS3215 (Orange)	EU	10%

17. DEDICATED EQUIPMENT

17.1. Dedicated Equipments are provided to Customer in private racks and shared racks. To protect the performance and integrity of the racks, Customer shall in respect of all Dedicated Equipment ensure that its consumption of electricty, network and the use of Dedicated Equipment resource including but not limited to storage devices, shall be fair and reasonable.

17.2. Customer's consumption of electricity, network and Dedicated Equipement resource shall be deemed not fair and not reasonable, if Customer's use exceeds the Basic Power (as agreed in the Contract Overview) or exceeds the intended use of network and Dedicated Equipment resource including storage devices in such a way that at Leaseweb's sole discretion it may affect the use of other Leaseweb's Customer in the shared rack and performance of other Infrastructure in the racks, or exceed the intended use of Dedicated Equipment resource thereby greatly reducing its lifetime.

17.3. Dedicated Equipments in shared racks, are provided to Customer in a rack shared with other Leaseweb's Customers and therefore Customer's consumption of electricity exceeding the Basic Powermay affect the performance such as latency, bandwidth and/or IOPS of the Dedicated Equipment in the shared racks. To protect the performance and integrity of the Dedicated Equipments, Customer shall ensure that its consumption of electricity, network and Dedicated Equipment resource shall be fair and reasonable.

18. CLOUD SERVICES

18.1. Compute Capacity of the Cloud Platform for the Public Cloud Services is provided to Customer on a shared basis. To protect the performance and integrity of the Cloud Platform, Customer shall, in respect of Public Cloud Service, ensure that its use of Compute Capacity shall be fair and reasonable.

18.2. Customer's use of Compute Capacity shall be automatically deemed not fair and not reasonable, if Customer's use exceeds Leaseweb's overbooking factor as determined in the Service Specifications in such a way that at Leaseweb's sole discretion it may affect the performance of other Infrastructure on the Cloud Platform.

19. CLOUD STORAGE SERVICES

19.1. Leaseweb offers Cloud Storage Services, a Cloud Storage components of the Cloud Platform ("**Cloud Storage Services**"), with different storage types, storage capacity and performance tiers, differentiated on IOPS per volume and latency assigned to each tier. The Cloud Storage Services are provided to Customer on a shared storage system, and therefore Customer's use of the Cloud Storage Services may affect the performance (such as latency, storage bandwidth and IOPS) of the storage system as a whole. The IOPS per volume are based on a usage profile of 4K block size with 70/30 read/write use ("**Usage Profile**"), by default.

19.2. To protect the performance and integrity of the Cloud Platform, Customer shall ensure that its use of the Cloud Storage Service shall be fair and reasonable in line with its Usage Profile. Other Usage Profiles are supported by Leaseweb, but they may lead to different IOPS performance results.

19.3. Customer's use of the Cloud Storage Services shall be deemed unfair and unreasonable, if the Cloud Platform usage is consistently deviating from the Usage Profile in such a way that it affects the performance of the Cloud Platform as a whole, to be solely determined by Leaseweb at its sole discretion based on its own information and tools. Consistent deviating use that is deemed to be unfair and unreasonable will result in additional Fees.

20. SHARED WEB HOSTING SERVICE

20.1. Leaseweb's Shared Web Hosting Platform is made available to Customer on a shared basis. To protect the performance and integrity of the Leaseweb Shared Web Hosting Platform, Customer shall ensure that its use of Shared Web Hosting Services shall be fair and reasonable.

20.2. Customer's use of the Shared Web Hosting Services shall be deemed unfair and unreasonable, if:

a) Customer uses the Shared Web Hosting Services in such a way that (in Leaseweb's reasonable opinion) it affects the performance of the Shared Web Hosting Platform or causes an Emergency;
b) the database size exceeds the total disk space allotted to Customer on the Shared Web Hosting Platform by 30%;
c) IMAP exceeds 5 connections per IP address;
d) twenty-five percent (25%) or more of the system resources are used in connection with Shared Web Hosting Services for longer than ninety (90) seconds at a time. Activities that could cause this excessive use include, but are not limited to, CGI scripts, FTP, PHP, HTTP; and/or
e) Customer runs any MySQL queries longer than twenty (20) seconds. MySQL tables should be indexed appropriately.

21. MULTI-CDN

21.1. The Multi-CDN Service is provided for Customer's consistent, fair and reasonable use.

21.2. Data Traffic Limits: Leaseweb reserves the right to limit the amount of Leaseweb Shield CDN Data Traffic passed through the Leaseweb Shield CDN to ensure the stability and reliability of our Network. If a Customer's Shield CDN Data Traffic exceeds 5% of the Monthly Committed Data Traffic, Leaseweb may (i) limit Customer's Leaseweb Shield CDN Traffic, (ii) purge the cache on Leaseweb Shield CDN AND/or (iii) disable Customer's Leaseweb Shield CDN setup to prevent disruption of other Customers' Multi-CDN Services.

21.3. Object size: Customer agrees and acknowledges that the Multi-CDN Services Fees are based upon an average object delivery size of 32KB or larger per HTTP/HTTPS request. Leaseweb reserves the right to charge Customer an additional Fee per 10.000 HTTP/HTTPS requests for Data Traffic with an average object of less than a 32KB.

21.4. The usage of the Leaseweb Shield CDN by Customer as a storage service is strictly prohibited.

21.5. The usage of the Multi-CDN Service by Customer shall be deemed inconsistent, unfair and/or unreasonable in the event (i) Customer exceeds the Leaseweb Shield CDN Traffic limits in Clause 15.2, or (ii) Customer's average object size is less than 32KB, and/or (iii) the Leaseweb Shield CDN is being used as a storage service.

21.6. In the event Leaseweb determines in its sole discretion, that Customer is not using the Multi-CDN Service in accordance with this Multi-CDN Fair Use Policy, Leaseweb shall be entitled to immediately impose limits on of the Data Traffic the Customer may transmit/receive through the Multi-CDN Service without any prior notice and Leaseweb shall be entitled to terminate the Multi-CDN Services.

CHAPTER E. SECURITY POLICY

22. INFRASTRUCTURE CONFIGURATION

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

22.2. 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.

22.3. Customer shall ensure that all data distributed through the Service shall be free of Viruses. Leaseweb 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.

23. MONITORING / REPORTING

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

23.2. Customer shall immediately report to Leaseweb's NOC any security-related event that may materially impact Leaseweb's Infrastructure, Leaseweb's organisation or Leaseweb's provision of services to other customers. Customer shall make the log in relation to such event

immediately available to Leaseweb upon Leaseweb's request, and shall follow any directions given by Leaseweb's as may be required to contain or correct the event.

CHAPTER F. FACILITY OPERATIONS POLICY

24. INTRODUCTION

24.1. The Facility Operations Policy contains a code of conduct for the day to day operations – and the presence of Customers – at a Data Center.

24.2. Leaseweb has adopted the Facility Operations Policy for the security and safety of Customers, Customer's employees, Customer's (sub)contractors and/or the Infrastructure.

25. SHIPMENTS

25.1. Each Customer shall observe the shipping and receiving policies adopted from time to time by Leaseweb with respect to shipment of Equipment to and from the Data Center.

25.2. Customer shall notify Leaseweb of any intended shipment to the Data Center, at least two (2) business days before the intended delivery date of the Equipment. Such notification will be given by Customer by means of the shipment notification form available in the Customer Portal. In relation to administrative activities performed by or on behalf of Leaseweb in connection with such shipment, Leaseweb shall be entitled to payment by Customer of a shipment charge in the amount of: (i) fifty Euros (€ 50,--), in the event that Customer has timely notified Leaseweb of the intended shipment; or (ii) two hundred and fifty Euros (€ 250,--), in the event that Customer has not notified or has not timely notified Leaseweb of the (intended) shipment.

25.3. All costs related to Customer's shipments of Equipment to or from a Data Center shall be at Customer's cost and expense.

25.4. Customer is responsible for cleaning up and disposal of all materials and equipment used for Customer's shipment. Customer shall ensure that such shipment material is removed from the Data Center on the same day as the date of delivery. If Customer does not comply with this provision, Leaseweb shall charge a clean up fee to Customer.

25.5. Customer shall use its own company name and Business information as receiver/importer reference for any Customer or Customer third party supplier's initiated shipment, import and/or transport and customs documentation for any packages or letters to the Data Center for receipt by the Customer. All shipments sent by Customer and/or by a Customer engaged third-party supplier to Customer at the Data Center shall be at Customer's own risk and expenses and Customer has the duty to fill properly fill out and submit all transportation and customers documentation accordingly. It is prohibited for the Customer to list or mention Leaseweb as receiving or importing party for such Customer or Customer third party supplier initiated Shipments. Leaseweb is not responsible for Customer's or Customer's Supplier initiated shipments to or from the Data Center. For the avoidance of doubt: Leaseweb cannot be used as importer of records by Customer of its Customer engaged third party supplier.

26. PHYSICAL STORAGE

26.1. Data Centers have little or no storage area. Leaseweb cannot assure the safety of Colocated Equipment that is not secured in the Housing Space or contained within the Data Center.

26.2. If Customer is not ready to install certain Equipment, and it is too bulky to contain within the Housing Space, Leaseweb may require Customer to store the Equipment in a storage area at Customer's expense.

27. CONDUCT AT DATA CENTER

27.1. With the exception of an Emergency, Customer with a 24/7 access card shall give Leaseweb at least one (1) hours' notice for access to the Data Center and/or Housing Space, and Customer without a 24/7 access card shall give Leaseweb at least twenty four (24) hours' notice for access to the Data Center and/or Housing Space.

27.2. Customer shall identify itself at the reception of the Data Center by showing a valid ID (Driver's license, Passport, Country ID) and explain the purpose of its visit. Customer is required to sign in and out when entering and exiting the Data Center, whereby Customer shall indicate its time of entry and time of exit. The reception will hand over an access card. Customer shall at all times during the visit wear the access card which needs to be fully visible. Before leaving, Customer shall - at the reception – hand in the access card; failure to do so may result in additional ServiceFees.

27.3. On a daily basis, Customer may allow a maximum of three (3) persons to access the Data Center. A Service Fees shall be due by Customer for each person entering the Data Center, with the exception of a holder of a 24/7 access card or those persons who are accompanying such card holder access card. Only the first person will be charged. Access shall be charged on a thirty (30) minutes interval basis, with a minimum of one (1) hour.

27.4. Customer shall provide Leaseweb with a list of persons authorized for access to the Housing Space and Colocated Equipment, which Customer may amend from time to time upon written notice to Leaseweb. Customer shall be responsible for all persons who receive access on behalf of Customer.

27.5. Leaseweb may require, at its sole discretion, that a Leaseweb representative escorts any representative of Customer accessing the Data Center and/or Housing Space. Also, the house rules of the Data Center may provide that the owner or lessor of the Data Center may - under certain circumstances - require that one of its staff escorts any representative of Customer who are accessing the Data Center and/or Housing Space.

27.6. If Leaseweb personnel provides an escort during Customer's access to the Data Center and/or Housing Space, such escort shall be considered an additional Service for which Leaseweb shall charge Customer an additional Service Fee (escort Fee) in addition to all escort Fees imposed on Leaseweb by the Data Center owner. If a representative of Customer is accompanied by an escort provided by the owner or lessor of the Data Center while accessing the Housing Space, Customer shall pay Leaseweb all related escort Fees that may be imposed on Leaseweb.

27.7. Customer shall (i) at all times, act in a professional manner, (ii) not interfere in any way with Leaseweb's use or operation of the Data Center or with the use or operation of any Equipment installed by other parties, including Equipment of other Customers. Should Customer require to (re)move or disconnect another party's Equipment to service its own Equipment, Customer shall contact Leaseweb and request Leaseweb's instructions prior to any such movement, removal and/or disconnection, taking into account a 48 hour notice period, (iii) refrain from operating any Equipment that may constitute a safety hazard, (iv) not perform any tests that may cause harm or damage to – or interfere with – the Leaseweb Network, the Housing Space and/or the Data Center, and (v) ensure that it closes doors after use, in order to maintain a closed and secure environment and thus ensuring an efficient environment for the fire protection system and climate control system, and (vi) lock the Rack before leaving. If in doubt, Customer shall consult the facility manager of the Data Center or – in the facility manager's absence – another employee of Leaseweb.

27.8. Leaseweb may at its sole discretion remove any of Customer's personnel or Customer's (sub)contractors or third party agents, if such person does not comply with any Leaseweb Policy, or any instruction provided by an employee of Leaseweb.

27.9. In case of an Emergency, such as a fire, which in general will be indicated by the sound (slow whoop) of an alarm system, Customer shall immediately evacuate the Data Center.

27.10. Smoking is prohibited in the entire Data Center. Eating and drinking is prohibited in the areas within the Data Center where the Housing Space and/or Equipment is located.

27.11. Within the areas where the Housing Space and/or Equipment is located, Customer shall refrain from any activity that may cause dust particles. One of the reasons for this prohibition, is that dust particles may set off the automatic alarm system. If in doubt, Customer shall consult the facility manager of the Data Center or – in the facility manager's absence – another employee of Leaseweb.

27.12. Unless expressly required under any (product)insurance warranty, Customer shall not bring any packaging material into the areas where the Housing Space and/or Equipment is located and any (card board) boxes shall be unwrapped by Customer in the loading bay area. Should Customer - in view of a (product)insurance warranty - require to bring packaging material into the areas where the Housing Space and/or Equipment is located, it will notify Leaseweb thereof in advance. Leaseweb will then assign a member of its staff to accompany Customer during Customer's presence in the areas where the Housing Space and/or Equipment is located. Customer is under an obligation to remove all packaging material from the areas where the Housing Space and/or Equipment is located, within one (1) hour after entering the relevant area.

27.13. Customer shall immediately report any irregularities and/or alarms, noticed by Customer during its presence in the Data Center, to the facility manager of the Data Center or – in the facility manager's absence – another employee of Leaseweb.

28. EQUIPMENT REQUIREMENTS

28.1. Unless expressly agreed otherwise in writing by Leaseweb, all Equipment shall be installed and maintained by or on behalf of Customer in accordance with the following criteria: (i) Telecommunication lines shall be extended from an organized and protected distribution frame; (ii) Spare parts for the Equipment shall be kept within the confines of the Housing Space; (iii) AC and DC power distribution shall take place within the Housing Space, to the extent available; (iv) Equipment density shall be consistent with floor loading at the Facility; (v) All cables shall be tied and harnessed in an orderly fashion; (vi) Equipment shall be in full compliance with telecommunications industry standards and in accordance with Leaseweb's requirements and specifications; (vii) all Colocated Equipment and associated cabeling shall be installed in such a way that the related cabinet can be closed and locked; and (viii) Equipment shall comply with applicable laws, rules and regulations in the jurisdiction where located and in addition as applicable in the EU (including specifically, but without limitation, the EU EMC Directive (89/336/EEC) and the EU Low Voltage Directive (73/23/EEC)), as amended from time to time.

28.2. Customer is expressly prohibited from installing any AC UPS Equipment in the Housing Space or at the Data Center in general.

28.3. Customer must ensure that Equipment with AC power supplies have a power factor of 0.85 or higher.

CHAPTER G. INVESTIGATION AND ENFORCEMENT POLICY

29. INVESTIGATION

29.1. Leaseweb 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 (including a Digital Services Coordinator), and reserves the right to take action based on the outcome of such investigation.

29.2. As part of this investigation, Leaseweb 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(s) Customer is obliged to fully cooperate with any such investigations by Leaseweb.

30. LEASEWEB'S ACTION(S)

30.1. To the extent legally required, Leaseweb is authorised to grant relevant law enforcement authorities (including a Digital Services Coordinator) access to Customer's content, information and/or Infrastructure, as well as any information gathered in the investigation conducted by Leaseweb this Chapter.

30.2. Upon request of a third party, a law enforcement authority (including a Digital Services Coordinator), Leaseweb shall be entitled to disclose identifying Customer information to said party in connection with a (suspected) breach of the Leaseweb Policies to the extent required by law (such to be determined in Leaseweb's discretion).

30.3. Leaseweb 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 Leaseweb, 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 records; and/or (j) placing files infected by Malicious Software in quarantine.

30.4. To enhance transparency and compliance with the DSA, Leaseweb may publish reports outlining its content moderation practices, including the number and nature of content removals and Customer accounts suspended or terminated.

30.5. Leaseweb herewith informs Customer that if Leaseweb becomes aware of any information giving rise to a suspicion that a criminal offence involving a threat to the life or safety of a person or persons has taken place, is taking place or is likely to take place, it shall promptly inform the law enforcement or judicial authorities of the Member State or Member States concerned of its suspicion and provide all relevant information available.

31. DISCLAIMER

31.1. Without prejudice to the above or any other provision of the Policies, Leaseweb does not intend to review, monitor or control as a precautionary measure content stored, sent or received by Customers using the Services. Accordingly, Leaseweb 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.

31.2. None of the provisions of this Chapter G or any of the other Chapters of the Policies shall in any way limit or prejudice any other rights or remedies Leaseweb may have.