

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 CDN Services and ancillary Services may be used by Customer and what manner of use is considered unacceptable by LeaseWeb. LeaseWeb's general terms and conditions (the "General Conditions"), LeaseWeb's service specification (the "Service Specification"), and LeaseWeb's Support and Service Level Schedule ("Support and Service Level Schedule"), are also part of the Agreement and apply to the CDN Services and ancillary Services provided by LeaseWeb.

CHAPTER A. INTRODUCTION

1. DEFINITIONS

- 1.1. In addition to the definitions set out in the General Conditions, the Support and Service Level Schedule and the Services Specification, the following definitions shall apply:

Authentication 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.

DDoS means Distributed-Denial-of-Service.

DoS means Denial-of-Service.

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

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.

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.

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

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

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.

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

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

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 LeaseWeb 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 CDN 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 Agreement or any applicable law.
- 5.2. Without prejudice to the law that applies to the Agreement, 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 Customer 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 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, zoophilia, child pornography, and child erotica; (xi) intentionally accessing a computer system or Infrastructure structure component without authorization or exceeding authorized access levels thereof; (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 LeaseWeb to Customer; and (xiii) 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 F of the LeaseWeb Policies and in the General Conditions.

6. INTERNET USE

- 6.1. Customer is prohibited from posting or transmitting unlawful material on or via the Internet or the World Wide Web.
- 6.2. 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.
- 6.3. 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 content. 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 the Agreement by sending a written notice to Customer.

7. USE OF THE CUSTOMER PORTAL

- 7.1. Subject to the terms of use applied from time to time by LeaseWeb Global B.V., and subject to the provisions of the Agreement, 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.
- 7.2. Customer shall observe each and any instruction of LeaseWeb Global B.V. regarding the use of the Customer Portal.

8. USE AND REGISTRATION OF (INTERNET) DOMAINS

- 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 an (Internet) domain, such as – for example – ICANN and SIDN.

CHAPTER C. ABUSE COMPLIANCE POLICY

9. ABUSE HANDLING REQUIREMENTS

- 9.1. In connection with use of LeaseWeb Services, Customer shall adopt and apply an abuse handling procedure which is compliant with the LeaseWeb Policies, with the law that applies to the Agreement and with any other law applicable to Customer.
- 9.2. 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.
- 9.3. 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.
- 9.4. Customer shall ensure the availability of sufficient and properly trained personnel to ensure that Customer’s End Users comply with the LeaseWeb Policies and to apply Customer’s abuse handling procedure and to handle the volume of abuse notifications that arrive without backlogs.

10. ABUSE PROCEDURE

- 10.1. If LeaseWeb 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”), LeaseWeb shall notify Customer hereof by way of email or such other method of communication as LeaseWeb deems appropriate.

- 10.2. 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.
- 10.3. 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.
- 10.4. 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 General 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.
- 10.5. Customer shall provide LeaseWeb with all documents and information in connection with the Abuse Notification without cost and on first demand.
- 10.6. 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.

11. REPEAT INFRINGERS AND LIVE VIDEO STREAMS

- 11.1. As part of its abuse handling procedure, Customer should make reasonable efforts to detect repeated efforts by its End Users to store or transfer or distribute – on or via Customer’s services – (i) materials or data that violate or infringe the Acceptable Use Policies; or (ii) that Customer previously deleted or disabled further to receipt of an Abuse Notification.
- 11.2. Customer shall immediately terminate the provision of service to an End User -and terminate an End User’s access to the Service- in the event that such End User is discovered to be a repeat infringer or violator of the LeaseWeb Acceptable Use Policies.
- 11.3. In the event Customer’s services are repeatedly used for streaming of live video and/or audio, Customer shall offer an online tool to trusted third parties (or their agents) to allow them to immediately terminate live video streams that are infringing on the intellectual property rights of these trusted third parties.

CHAPTER D. FAIR USE POLICY

12. FAIR USAGE

- 12.1. The Service is provided for Customer’s consistent, fair and reasonable use.
- 12.2. Usage of the Service shall deemed inconsistent, unfair and/or unreasonable use in the following events: (i) Customer’s total Data Traffic usage in any 5 minute period exceeds 500% of the monthly Committed Data Traffic divided by 8,712; or (ii) Customer’s average Bandwidth usage for any 5 minute period exceeds 500% of the monthly Committed Bandwidth.
- 12.3. Usage of the Service shall deemed inconsistent, unfair and/or unreasonable use in the event the CDN Traffic is not following the natural ASN distribution of the audience of Customer content but is artificially concentrated in one or several specific ASN(s) or regions.
- 12.4. In the event LeaseWeb, in its sole discretion, determines that the Customer is not using the Service according to this Fair Use Policy, LeaseWeb will, without any prior notice, be entitled to immediately impose limits on the speed of the data the Customer may transmit and/or receive through the Service.
- 12.5. Should the total size of Popular Hot Content be repeatedly over 20TB, then the highest volume in excess of said 20TB threshold shall be charged EUR 2 /GB per month additionally, unless payment of Service Charges in another currency is agreed between Parties, in which case the excess charge shall be payable in that other currency and the amount of that excess charge shall be the equivalent in that currency of 2 EUR/GB per month.
- 12.6. If in any calendar month, the Hit Factor exceeds 1000, LeaseWeb shall be entitled to charge Customer an addition Service Charge of EUR 0.25 per 1 million Hits that have occurred in the respective month, unless payment of Service Charges in another currency is agreed between Parties, in which case the excess charge shall be payable in that other currency and the amount of that excess charge shall be the equivalent in that currency of EUR 0.25.
- 12.7. 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 Traffic in excess of the ASN Threshold shall be charged at \$1,00 / Mbps on top of the normal rate (or the equivalence thereof if parties agreed on Services Charges in another currency).

Table 1: ASN Thresholds

ASN DESTINATION	REGION	ASN THRESHOLD
AS701 (Verizon)	US	3%
7922 (Comcast)	US	7%,
20115 (Charter)	US	2%
28573 (Brasil)	US	4%
7018 (AT&T)	US	3%
AS9121 (Turktelecom)	EU	2%
AS3320 (DTAG)	EU	2%
AS5089 (Virgin)	EU	2%
AS3352 (Telefonica)	EU	2%
AS3215 (FT)	EU	2%
AS4134 (China Telecom)	AP	1%
AS4837 (China Unicom)	AP	1%

CHAPTER E. SECURITY POLICY

13. INFRASTRUCTURE CONFIGURATION

- 13.1. Customer is advised to back-up (critical) data and system configurations on a regular basis and store such data in a safe place
- 13.2. 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.

14. MONITORING / REPORTING

- 14.1. Customer shall implement logging and monitoring measures for security-related events.
- 14.2. 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. INVESTIGATION AND ENFORCEMENT POLICY

15. INVESTIGATION

- 15.1. LeaseWeb reserves the right to conduct an investigation, based on (i) suspected violations of the LeaseWeb Policies; and/or (ii) (potential) security risks to its Infrastructure; and/or (iii) a valid request of the relevant (law enforcement) authorities.
- 15.2. 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 referenced in Clause 14. Customer is obliged to fully cooperate with any such investigations by LeaseWeb.

16. LEASEWEB ACTION

- 16.1. To the extent legally required, LeaseWeb 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 LeaseWeb under clause 15.1.
- 16.2. Upon request of a third party, LeaseWeb shall be entitled to disclose identifying Customer information to said party in connection with a (suspected) breach of the LeaseWeb Acceptable Use Policies to the extent required by law (such as to be determined in LeaseWeb's discretion).
- 16.3. LeaseWeb shall be entitled to take action, legal or otherwise, against Customer and/or End User, in the event that the use of the Service by Customer or its End User(s), breaches the LeaseWeb Policies, or Customer fails to comply with any obligation under the LeaseWeb 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 General 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 to Customer's content; (g) denying Customer (physical) access to Infrastructure; (h) providing binding instructions to Customer in regards of the use of the Services, and/or (i) placing files infected by Malicious Software in quarantine.

17. DISCLAIMER

- 17.1. Without prejudice to the above or any other provision of the LeaseWeb Policies, LeaseWeb does not intend to review, monitor or control as a precautionary measure content 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.
- 17.2. None of the provisions of this Chapter F or any of the other Chapters of the LeaseWeb Policies shall in any way limit or prejudice any other rights or remedies LeaseWeb may have.