LEASEWEB POLICIES

TABLE OF CONTENTS

CLAUSE PAGE

CHAPTER 1: INTRODUCTION

1 DOCUMENT STRUCTURE / INTERPRETATION

1.1 LeaseWeb and Customer have entered into an agreement with respect to the provision of Services by LeaseWeb to Customer (the **"Agreement"**). The LeaseWeb Policies are part of the Agreement and shall apply to the Services provided by LeaseWeb.

1.2 LeaseWeb's description and specification of its Services (the **"Services Specification"**), LeaseWeb´s description and specification of the available Service Levels (the **"Service Level Schedule"**) and LeaseWeb's general terms and conditions (the **"General Conditions"**) are also part of the Agreement and apply to the Services and any Equipment provided by LeaseWeb.

1.3 The provisions of the Services Specification, the Service Level Schedule and the General Conditions, including the definitions used therein, shall apply to the LeaseWeb Policies. In the event of a discrepancy or a dispute between any of the provisions of the LeaseWeb Policies and any of the provisions of the Services Specification, the Service Level Schedule or the General Conditions, such will be resolved in the manner specified in the General Conditions regarding the order of precedence.

1.4 In addition to the definitions set out in the General Conditions, the following definitions shall apply:

Blacklist	means a so called blacklist or block list which is a basic access control system that denies entry or access to a specific list or range of users or network addresses or IP addresses, as a result of which e-mail sent by a user or from a network address or from an IP address that is on the blacklist will not reach its intended destination or recipient
DoS	means Denial-of-Service
Disruption	for the purpose of Clause 3 (Usenet news Use) of Chapter 2 (Acceptable Use Policy), means posting a large number of messages to a newsgroup, which contain no substantive content, to the extent that normal discussion in the group is significantly hindered. Examples of disruptive activities include, but are not limited to, posting multiple messages with no text in the body, or posting many follow-ups to messages with no new text
DDoS	means Distributed-Denial-of-Service
DRDoS	means Distributed-Reflected-Denial-of-Service
Hardware	means the physical part of the Equipment
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
IETF	means the Internet Engineering Task Force which is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet
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
Netiquette	means the established Usenet conventions
Operating System	means the Software on a computer that manages the way different programs use the Hardware, and regulates the ways that a user controls the computer
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*)
SNMP	means Simple Network Management Protocol, i.e. an Internet-standard protocol for managing devices on IP networks
Spam	means unsolicited broadcast e-mail or unsolicited commercial e-mail that is sent to addresses that do not affirmatively and verifiably request such material from that specific sender, including but not limited to advertising, surveys, information pieces, third party spamming, website addresses, sales, and auctions
SSC	means LeaseWeb's Self Service Center
Usenet	means the global Internet discussion system
Virus	means any type or form of malicious-, hostile-, intrusive- or annoying Software, including but not limited to computer viruses, worms, trojan horses, spyware and dishonest adware
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 among other the use of the Internet and the use of E-mail. For this purpose, LeaseWeb has created the LeaseWeb Policies.

2.2 In the LeaseWeb Policies are set out the policies and guidelines applied by LeaseWeb 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 LeaseWeb.

2.3 All Customers must read and comply with the LeaseWeb Policies and, where Customer provides services to its own clients, Customer is required to ensure that its clients are aware of and comply with the LeaseWeb Policies, as though such client were a Customer.

2.4 A Breach of the LeaseWeb Policies by a person or (legal) entity who obtains access to Services via a Customer will also be considered a Breach of the LeaseWeb Policies by that Customer.

2.5 LeaseWeb provides all of its Customers with a copy of the LeaseWeb Policies, prior to or upon entering into an agreement with a Customer.

3 LEASEWEB POLICIES

3.1 The LeaseWeb Policies consist of:
3.1.1 the Acceptable Use Policy;
3.1.2 the Security Policy;

3.1.3 the Facility Operations Policy; and
3.1.4 the Equipment Policy.

3.2 LeaseWeb reserves the right to unilaterally update or change or amend the LeaseWeb Policies in accordance with the provisions of the General Conditions.

CHAPTER 2: ACCEPTABLE USE POLICY

1 USE OF SERVICES

1.1 Customers shall only use the Services for lawful purposes and shall refrain from any use that Breaches the LeaseWeb Policies, the General Conditions, the Services Specification, the Service Level Schedule, the Agreement or any applicable Law.

1.2 Without prejudice to the generality of Clause 1.1 of this Chapter 2, and without prejudice to the law that applies to the Agreement, the Customer acknowledges and agrees that the Customer's use of the Services is to be compliant with (mandatory) Law in the country where the Equipment is located; and that LeaseWeb shall be entitled to vary the Service in order to comply with such local Law.

1.3 Specific activities that are prohibited include, but are not limited to:
1.3.1 threatening harm to persons or property or otherwise harassing behaviour;
1.3.2 compromising the security or tampering with system resources or accounts of other Customers or of any other Internet sites or intranet sites networks, private- or public domains;
1.3.3 violating local export control Laws for Software or technical information;
1.3.4 the use or transmission or distribution of any data or material protected by copyright, trademark, trade secret, patent or other Intellectual Property Right without proper authorisation;
1.3.5 the manufacture or use or distribution of counterfeit, pirated or illegal software or other product;
1.3.6 fraudulently representing products or services;
1.3.7 Spamming, hacking, DoS attacks, DDoS attacks, DRDoS attacks;
1.3.8 defamation, child pornography, child erotica and obscenity;
1.3.9 facilitating, aiding, or encouraging any of the above activities;
1.3.10 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.

1.4 Customer acknowledges that any use of the Services in Breach of the Acceptable Use Policy could subject Customer to criminal and/or civil liability, in addition to other actions by LeaseWeb outlined in Chapter 6 of the LeaseWeb Policies and in the General Conditions.

2 USE OF MATERIAL

2.1 Subject to the other provisions of the LeaseWeb Policies, Customer shall when using the Services be entitled to download or upload or re-distribute materials that are in the public domain (e.g., images, text, and programs). Whether or not materials are in the public domain shall be determined by Customer and Customer shall bear all risks and liabilities regarding the use of such material and the determination of whether the material used is in the public domain.

2.2 Customer is prohibited from storing, distributing or transmitting any unlawful material through the Services. Examples of unlawful material include, but are not limited to:
2.2.1 direct threats of physical harm;

2.2.2 child pornography, child erotica; and
2.2.3 copyrighted, trademarked and other proprietary material used without proper authorization or consent of the party that holds legal title to such material.

2.3 Customer may not store or distribute certain other types of material. Examples of such prohibited material include, but are not limited to:
2.3.1 programs containing Viruses;
2.3.2 tools to compromise the security of other Internet sites, intranet sites, networks, private or public domains. Examples of these tools include, but are not limited to, password guessing programs, cracking tools or network probing tools;
2.3.3 tools used to collect e-mail addresses for use in sending bulk e-mail; or
2.3.4 tools used to send bulk mail.

2.4 Customer acknowledges that the storage, distribution, or transmission of unlawful or prohibited materials could subject Customer to criminal and/or civil liability, in addition to other actions by LeaseWeb outlined in Chapter 6 of the LeaseWeb Policies and in the General Conditions.

3 USENET NEWS USE

3.1 Subject to the provisions of this Acceptable Use Policy, Customer is entitled to access and use Usenet through the Services or the Network.

3.2 Usenet news articles posted by Customer or Customer's clients with the use of the Services must comply with the written charter/FAQ of the newsgroup to which they are posted. If a newsgroup does not have a charter or FAQ, its title may be considered sufficient to determine the general topic of the newsgroup.

3.3 Netiquette prohibits advertising in most Usenet newsgroups. Customer may post advertisements only in those newsgroups that specifically permit the posting of advertisements in their charter or FAQ. Some newsgroups may permit so called 'classified ads' for single transactions between private individuals, but not commercial advertisements.

3.4 Netiquette prohibits certain types of posts in most Usenet newsgroups. Types of prohibited posts include chain letters, pyramid schemes, encoded binary files, job offers or listings and personal ads.

3.5 Only the poster of a Usenet article or LeaseWeb has the right to cancel the article. Customer may not use LeaseWeb's resources to cancel articles that were not posted by or on behalf of Customer. The sole exception to this rule is for moderators of formally moderated newsgroups; the moderator of a newsgroup may cancel any articles in a newsgroup he or she is moderating.

3.6 Customer may not (whether directly or through others) 'flood' or cause a Disruption of Usenet newsgroups, or attempt to flood or cause a Disruption of Usenet newsgroups.

3.7 Customer may not alter the headers of posts to Usenet to conceal his e-mail address or to prevent Customer from responding to posts.

3.8 Customer is responsible for determining the rules of a newsgroup before posting to it. As such, Customer is responsible for determining whether or not a newsgroup permits a type of message before posting and whether or not a newsgroup permits advertisements before posting.

4 E-MAIL USE / ANTI-SPAM

4.1 LeaseWeb recognizes that e-mail is an informal medium. On the other hand, LeaseWeb is very much aware of the existence of misuse of e-mail. Such misuse is prohibited by LeaseWeb.

4.2 Customer may not send e-mail that in any way is or may be in Breach of applicable Law.

4.3 Customer shall refrain from any e-mail activities that may result in the placement of Customer or Customer's IP address(es) on a Blacklist. LeaseWeb reserves the right charge Customer 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, LeaseWeb's servers or IP address(es) are placed in any third-party mail filtering software or Blacklist.

4.4 Customer shall refrain from sending further e-mail to a recipient of its e-mail after receiving a request to stop from such recipient.

4.5 Unsolicited advertising mailings, whether commercial or informational, are strictly prohibited. Customer may send advertising material only to recipients that have specifically requested that material. Opt-out mailings are, in view of the foregoing, prohibited.

4.6 Customer may not send or propagate Spam and shall not allow its clients or third parties to send or propagate Spam via Customer's IP addresses.

4.7 Customer may not send, propagate, or reply to Mail Bombs and shall not allow its clients or third parties to send or propagate Mail Bombs via Customer's IP addresses.

4.8 Customer may not alter the headers of e-mail messages to conceal Customer's e-mail address or to prevent receivers from responding to messages.

5 WORLD WIDE WEB USE

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

5.2 For the purpose of this Clause, inappropriate material shall include the examples set in Clause 2.2 and Clause 2.3 of the Acceptable Use Policy.

5.3 LeaseWeb from time to time actively blocks 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 IRC USE

6.1 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.

6.2 For the purpose of this Clause, inappropriate material shall include the examples set in Clause 2.2 and Clause 2.3 of the Acceptable Use Policy. Other examples of prohibited use of IRC are so called 'eggdrops' and 'psybnc shell hosting'.

7 USE AND REGISTRATION OF (INTERNET) DOMAINS

7.1 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.

8 USE AND REGISTRATION OF IP ADDRESSES AND AS NUMBERS

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

9 USE OF THE SSC

9.1 Subject to the other provisions of the LeaseWeb Policies, Customer shall be entitled to use the SSC.

9.2 Use of the SSC by or on behalf of Customer shall be at Customer's risk and responsibility.

9.3 Customer shall limit its use of the SSC to the requirements of the ordinary course of its business.

9.4 Customer shall observe each and any instruction of LeaseWeb regarding the use of the SSC.

10 ABUSE CONTACT PERSON(S)

10.1 Customer shall designate one or more person(s) whom LeaseWeb may contact at any time in connection with (suspected) violations by Customer of the LeaseWeb Policies. Customer will provide to LeaseWeb a means of contacting such person(s) at any and all times.

CHAPTER 3: SECURITY POLICY

1 INTRODUCTION

1.1 Security is as important to LeaseWeb as it is to its Customers. For this reason, LeaseWeb has established standards and information security requirements for all networks and Equipment deployed in a LeaseWeb Datacenter and the Network, including standards for the basic configuration of Equipment, the use of passwords and the use of effective virus detection and prevention.

1.2 The Security Policy is intended to minimise the risk of damage loss of or damage to Equipment, loss of or damage to or unauthorised use of data or technology, unauthorised use of confidential information, loss of or damage to or unauthorised use of Intellectual Property Rights.

1.3 In addition to the guidelines and policies set out in this Security Policy, all Customers must read and comply with the requirements and the recommendations outlined in the so called 'Site Security Handbook', made available by IETF on its website (**www.ietf.org**) under reference number RFC2196, and such other applicable security requirements and recommendations published by IETF from time to time.

2 EMERGENCY CONTACT / REGISTRATION REQUIREMENTS

2.1 Customer shall designate one or more person(s) whom LeaseWeb may contact at any time in the event of an Emergency or otherwise as needed by LeaseWeb. Customer will provide to LeaseWeb a means of contacting such person(s) at any and all times.

2.2 Any Co-located Equipment shall be registered by Customer in SSC on the Effective Date. At a minimum, Customer shall provide the following information:

2.2.1 Server contact(s) and location, and a backup contact;
2.2.2 Hardware (brand, version and number of servers);
2.2.3 Operating System (brand and version);
2.2.4 Main functions and applications (if applicable).

2.3 Customer shall ensure that the information set out in SSC with respect to Customer and its Equipment is up to date.

3 BASIC EQUIPMENT CONFIGURATION

3.1 Customer should preferably have its Equipment installed and housed in a physically separate room from any other networks and Equipment. As a minimum, the Equipment should be installed and kept in a locked rack, with limited access. In addition, Customer shall provide LeaseWeb with a list of persons who shall be entitled to access to Customer's Equipment.

3.2 Customer should back-up (critical) data and system configurations on a regular basis and store such data in a safe place.

3.3 Production resources should not be used for testing and/or development purposes.

3.4 Customer shall not connect its Equipment via a wireless connection.

3.5 Customer should (where practical) disable services and applications that are not used by Customer.

3.6 Customer should, to the extent possible, log and protect access to the Services through access control methods such as so called TCP Wrappers.

3.7 Customer should avoid using so called trust relationships between systems, in the event that another method of communication is available.

3.8 Customer should always use standard security principles of least required access to perform a function.

3.9 Customer should not use 'root' in the event that a non-privileged will do.

3.10 If a methodology for secure channel connection is available (i.e. technically feasible), Customer should ensure that privileged access is performed over secure channels (e.g. encrypted network connections using 'secure shell' or 'Internet Protocol security').

3.11 Customer shall ensure that its Equipment can not and does not operate from uncontrolled networks.

4 PASSWORDS / PASSPHRASES

4.1 LeaseWeb shall provide Customer with a login and a password for LeaseWeb's portal. This login and password allows access to Customer's account and Equipment and may be used to request support or other Services. Also, LeaseWeb's technical support staff will ask for Customer's login and password in case of a support issue or Emergency, in order to authenticate Customer.

4.2 Customer is required to change its password the moment it starts using the Services or its Equipment is activated and Customer is responsible for changing the password regularly. In general, secure passwords are between six (6) and eight (8) characters long, contain letters of mixed case and non-letter characters, and cannot be found in whole or in part, in normal or reverse order, in any dictionary of words or names in any language.

4.3 Customer shall arrange that all system-level passwords (e.g. root, enable, NT admin, etc.) are changed – at least – every three (3) months.

4.4 Customer shall arrange that all user-level passwords (e.g. e-mail, desktop computer, etc.) are changed – at least – every six (6) months.

4.5 Customer shall arrange that user accounts that have system-level privileges granted through group memberships or programs (e.g. 'sudo') have a unique password from all other accounts held by such user.

4.6 Customer shall ensure that passwords are not inserted into e-mail messages or other forms of electronic communication, except in its support requests or trouble tickets to LeaseWeb. In the event that a password has been inserted in an electronic communication, Customer shall arrange that such password is changed without undue delay.

4.7 In the event Customer uses SNMP, Customer shall ensure that (i) the community strings are defined as something other than the standard defaults of 'public', 'private' and 'system', and are different from the passwords used to log in interactively; and (ii) a 'keyed hash' is used where available (e.g. SNMPv2).

4.8 Clause 4.3 until Clause 4.8 shall also apply in the event that Customer uses passphrases in stead of or as well as passwords.

5 ANTI-VIRUS

5.1 Each Customer shall ensure that the Software operated or used on the Equipment is up to date, and accordingly that updates and patches are installed on a regular basis, without undue delay after becoming available.

5.2 Each Customer shall ensure that adequate anti-Virus Software is operated or used on the Equipment, and that such anti-Virus Software is used to scan the Equipment for Viruses at regular intervals (at least on a daily basis).

5.3 Any Equipment found to be infected with a Virus is to be (temporarily) disconnected from the Network, until the Virus has been removed and the infection has been cured.

5.4 In addition to the foregoing, in order to minimise the risk of Virus infections, LeaseWeb recommends that each Customer complies with the following processes:

5.4.1 Never open any files or macros attached to an e-mail from an unknown, suspicious or untrustworthy source;

5.4.2 Immediately delete the e-mail, including the files or macros, referred to in Clause 5.4.1, then empty the trash and subsequently remove the items from any restore-list;
5.4.3 Delete SPAM, in the manner specified in Clause 5.4.2;
5.4.4 Never download files from unknown or suspicious or untrustworthy sources;
5.4.5 Avoid direct disk sharing with read/write access unless – and to the extent that – there is an absolute necessity to do so;
5.4.6 Always scan any data and/or data storage medium obtained from an unknown- or unverified source for Viruses before using such data or data storage medium.

6 MONITORING / REPORTING

6.1 Customer shall log all security-related events on critical or sensitive systems, and save the related audit trails, in the following manner:
6.1.1 All security related logs shall be kept online for at least one (1) week;
6.1.2 Daily incremental tape backups shall be retained for at least one (1) month;
6.1.3 Weekly full tape backups of logs shall be retained for at least one (1) month;
6.1.4 Monthly full backups shall be retained for a minimum of two (2) years.

6.2 Customer shall immediately report any security-related event to LeaseWeb's NOC and follow any directions given by LeaseWeb's NOC as may be required to contain or correct the event.

6.3 For the purpose of this Clause 6, security-related events shall include, but not be limited to,:
6.3.1 Port-scan attacks;
6.3.2 unauthorised access to privileged accounts; and
6.3.3 anomalous occurrences that are not related to specific applications on the host.

CHAPTER 4: FACILITY OPERATIONS POLICY

1 INTRODUCTION

1.1 The Facility Operations Policy contains a code of conduct for the day to day operations – and the presence of Customers – at a LeaseWeb Datacenter.

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

2 SHIPMENTS

2.1 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 LeaseWeb Datacenter.

2.2 Customer shall notify LeaseWeb of any intended shipment to the LeaseWeb Datacenter, 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 SSC. 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.

2.3 Customer shall inform LeaseWeb, and the security personnel at the LeaseWeb Datacenter, of the Equipment Customer intends to bring into, install in or remove from the LeaseWeb Datacenter.

2.4 All costs related to Customer's shipments of Equipment to or from a LeaseWeb Datacenter shall be at Customer's cost and expense.

2.5 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 LeaseWeb Datacenter 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.

2.6 LeaseWeb does not accept any responsibility for shipments to or from the LeaseWeb Datacenter. All shipments made or sent by Customer shall be at Customer's own risk.

3 CONDUCT AT LEASEWEB DATACENTER

3.1 With the exception of an Emergency, Customer shall give notice to LeaseWeb at least twenty four (24) hours prior to visiting an LeaseWeb Datacenter.

3.2 Access to the LeaseWeb Datacenter, specifically the areas where the Housing Space is located, is limited to authorised LeaseWeb employees and Qualified Staff.

3.3 Customer is required to sign in and out when exiting and entering the LeaseWeb Datacenter, whereby Customer shall indicate its time of entry and time of exit.

3.4 When entering or exiting the LeaseWeb Datacenter, Customer shall use the secure access point installed from time to time by LeaseWeb or the operator or owner of LeaseWeb Datacenter.

3.5 Each visitor of the LeaseWeb Datacenter is required to wear his/her (personal) access card and shall be able to provide LeaseWeb with official identification papers (e.g. passport or drivers licence) at all times during his/her presence at the LeaseWeb Datacenter.

3.6 When inside the LeaseWeb Datacenter, Customer shall 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.

3.7 LeaseWeb may (at its discretion) accompany Customer inside the LeaseWeb Datacenter and LeaseWeb may (at its discretion) remain with Customer for the entire time that Customer is inside the LeaseWeb Datacenter.

3.8 Customer shall not interfere in any way with LeaseWeb's use or operation of the LeaseWeb Datacenter or with the use or operation of any Equipment installed by other parties, including Equipment of other Customers.

3.9 Customer shall refrain from any actions that may damage the Housing Space or the LeaseWeb Datacenter or any Equipment of a third party, including Equipment of other Customers.

3.10 Customer shall refrain from operating any Equipment that may constitute a safety hazard. If in doubt, Customer shall consult the facility manager of the LeaseWeb Datacenter or – in the facility manager's absence – another authorised employee of LeaseWeb.

3.11 Customer shall, at all times, act in a professional manner. 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 the Facility Operations Policy or any other LeaseWeb Policy.

3.12 In case of an Emergency, such as a fire, which in general will be indicated by the sound (slow woop) of an alarm system, Customer shall immediately evacuate the LeaseWeb Datacenter.

3.13 Smoking is prohibited in the entire LeaseWeb Datacenter. Eating and drinking is prohibited in the areas within the LeaseWeb Datacenter where the Housing Space and/or Equipment is located.

3.14 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 LeaseWeb Datacenter or – in the facility manager's absence – another authorised employee of LeaseWeb.

3.15 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.

3.16 Before exiting the LeaseWeb Datacenter, Customer shall ensure that its Housing Space is closed and locked.

3.17 Customer shall immediately report any irregularities and/or alarms, noticed by Customer during its presence in the LeaseWeb Datacenter, to the facility manager of the LeaseWeb Datacenter or – in the facility manager's absence – another authorised employee of LeaseWeb.

CHAPTER 5: EQUIPMENT POLICY

1 EQUIPMENT REQUIREMENTS

1.1 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:

1.1.1 Telecommunication lines shall be extended from an organized and protected distribution frame;
1.1.2 Spare parts for the Equipment shall be kept within the confines of the Housing Space;
1.1.3 AC and DC power distribution shall take place within the Housing Space, to the extent available;
1.1.4 Equipment shall include all necessary fans and ventilation;
1.1.5 Equipment density shall be consistent with available Electricity Supply;
1.1.6 Equipment density shall be consistent with floor loading at the Facility;
1.1.7 Grounding facilities shall be included;

1.1.8 All cables shall be tied and harnessed in an orderly fashion, run to the side of the rack, and labelled;
1.1.9 Connectors shall be secured in the interface socket;
1.1.10 All Equipment shall be suitably labelled as belonging to Customer, including any safety notices and instructions for Emergency repairs and /or contacts;
1.1.11 A copy of all records and documents relating to the Equipment shall be available for safe storage in the Housing Space, with Customer separately holding a complete set of such information at its premises;
1.1.12 Equipment shall be in full compliance with telecommunications industry standards and in accordance with LeaseWeb's requirements and specifications; and
1.1.13 Equipment shall comply with applicable laws, rules and regulations in the jurisdiction where located (including specifically in Europe, but without limitation, the EU EMC Directive (89/336/EEC) and the EU Low Voltage Directive (73/23/EEC)).

1.2 Customer is expressly prohibited from installing any AC UPS Equipment in the Housing Space or at the LeaseWeb Datacenter in general.

1.3 Equipment with AC power supplies shall have a power factor of 0.85 or higher.

2 ACCESS AND REPAIRS

2.1 LeaseWeb will not touch, maintain, use, upgrade, repair or operate Colocated Equipment,:
2.1.1 unless expressly authorized and instructed otherwise by Customer; and
2.1.2 except as required and possible in an Emergency.

2.2 LeaseWeb is entitled to access Housing Space, if such access is needed:
2.2.1 during an Emergency;
2.2.2 during a Service Disruption;
2.2.3 to perform Maintenance;
2.2.4 for security purposes; and
2.2.5 to perform an investigation or to enforce the LeaseWeb Policies in accordance with Chapter 6.

2.3 Customer shall designate one or more person(s) whom LeaseWeb may contact at any time in the event of an Emergency or otherwise as needed by LeaseWeb. Customer will provide to LeaseWeb a means of contacting such person(s) at any and all times.

CHAPTER 6: INVESTIGATION AND ENFORCEMENT (NOTICE & TAKEDOWN)

1 INVESTIGATION

1.1 LeaseWeb reserves the right to investigate (potential) security risks to its Network. As part of its investigation, LeaseWeb may – for example – review and investigate Customer's security log, as referred to in Clause 6 of Chapter 3.

1.2 LeaseWeb reserves the right to investigate suspected violations of the LeaseWeb Policies. LeaseWeb will investigate complaints and may, in its sole discretion, take action based on the rules below.

1.3 When LeaseWeb becomes aware of possible violations, as part of its investigation, LeaseWeb may – acting reasonably and providing Customer with information on (the grounds for) LeaseWeb's investigation –:
1.3.1 gather information from Customer involved;
1.3.2 gather information about Customer involved;

1.3.3 if relevant, gather information from a complaining party;
1.3.4 block access at the router and/or switch level to Customer's Equipment;
1.3.5 deny Customer (physical) access to its Equipment;
1.3.6 in view of the above, request Customer's login and a password to the Equipment for audit purposes.

1.4 Customer shall grant LeaseWeb any information and – further to a request of the relevant (Law enforcement) authorities to LeaseWeb or Customer – access to its Equipment required by LeaseWeb in order to perform its investigation.

2 ENFORCEMENT

2.1 If according to LeaseWeb' findings any of the LeaseWeb Policies has been Breached, LeaseWeb shall be entitled to take responsive action, legal or otherwise, against Customer and/or Customer's client or other person responsible for the Breach of the LeaseWeb Policies.

2.2 What action is appropriate will be determined by LeaseWeb from time to time, in its sole discretion, and may for example include:
2.2.1 suspension or termination of any or all of the Services;
2.2.2 suspension or termination of the Service Levels;
2.2.3 (selective) IP port-blocking;
2.2.4 a reinstall of the server(s); and/or
2.2.5 termination of the Agreement.
Other examples of actions that may be taken by LeaseWeb are set out below in Clause 2.3.

2.3 If LeaseWeb is notified by a third party, including any Law enforcement authority, of a (suspected) Breach by Customer of any of the LeaseWeb Policies, LeaseWeb shall be entitled to release any contact information with respect to Customer to such party, in order to assist that third party in resolving security incidents.

3 DISCLAIMER

3.1 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 all content sent or received by Customers using the Services. Accordingly LeaseWeb accepts no responsibility or liability to Customers or any other person for the content of any communications that are transmitted by or made available to Customers or their users, regardless of whether they originated from the Network or the Services.

3.2 None of the provisions of this Chapter 6 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.

- *** -