HOSTING SOLUTIONS

ACCEPTABLE USE POLICY (AUP)

1. SERVICE AGREEMENT

3W INFRA and CUSTOMER have executed a Service Agreement (the "Agreement"). The Parties agree that the terms and conditions of the Agreement govern this document. In the event of any conflict between the terms of this document and the Master Service Agreement, the Master Service Agreement shall control. Capitalized terms used in this document shall have the same meaning as in the Master Service Agreement and vice versa unless otherwise defined herein.

3W INFRA reserves the right to unilaterally amend the conditions set out in the Acceptable Use Policy (the "Policies").

2. USE OF SERVICES

2.1 CUSTOMER agrees to use 3W INFRA's Services only for lawful purposes, in compliance with all applicable laws.
2.2 Specific Activities that are prohibited include, but are not limited to:

- Threatening harm to persons or property or otherwise harassing behavior;
- Violating Dutch export control laws for software or technical information;
- Fraudulently representing products/services using your account;
- Facilitating, aiding, or encouraging any of the above activities;
- Spamming, hacking, DoS attacks.

2.3 Additional Activities are prohibited that appear in further sections of this AUP, including Article 3 (Use of Material) and 4 (System Security).
2.4 3W INFRA reserves the right to investigate suspected violations of this AUP. When 3W INFRA becomes aware of possible violations, 3W INFRA may initiate an investigation that may include gathering information from CUSTOMER involved and the complaining party.
2.5 During an investigation, 3W INFRA may block access at the router and/or switch level to CUSTOMER's equipment involved. 3W INFRA may also deny CUSTOMER's physical access to CUSTOMER's Equipment in the Data Center. If 3W INFRA believes, in its sole discretion, that a violation of this AUP has occurred, it may take responsive action. Such action may include, but is not limited to, temporary or permanent blocking of access to CUSTOMER's equipment, denying CUSTOMER's physical access to CUSTOMER's Equipment and the suspension or termination of CUSTOMER's Services.
2.6 3W INFRA, in its sole discretion, will determine what action will be taken in response to a violation on a case-by-case basis. Violations of this AUP could also subject CUSTOMER to criminal or civil liability.
2.7 CUSTOMER of record is responsible for all use of the Services, with or without the knowledge or consent of CUSTOMER.
2.8 3W INFRA staff will ask for the login and a password in case of a suspected violation by CUSTOMER. CUSTOMER shall give 3W INFRA access to CUSTOMER's Equipment, for audit purposes.
2.9 When entering the Data Center, CUSTOMER must uphold the Facility Rules & Regulations. These are made available on-premises and can be provided upon request by 3W INRRA.

3. USE OF MATERIAL

3.1 Materials in the public domain (e.g., images, text, and programs) may be downloaded or uploaded using 3W INFRA services. CUSTOMER may also re-distribute materials in the public domain. CUSTOMER assumes all risks regarding the determination of whether the material is in the public domain.

3.2 CUSTOMER is prohibited from storing, distributing or transmitting any unlawful material through 3W INFRA's services. Examples of unlawful material include but are not limited to direct threats of physical harm, child pornography, and copyrighted, trademarked and other proprietary material used without proper authorization. CUSTOMER may not post, upload or otherwise distribute copyrighted material on 3W INFRA's or CUSTOMER's Equipment without the consent of the copyright holder. The storage, distribution, or transmission of unlawful materials could subject CUSTOMER to criminal as well as civil liability, in addition to the actions outlined above.

3.3 CUSTOMER may not store or distribute certain other types of material. Examples of prohibited material include, but are not limited to, programs containing viruses or Trojan horses and tools to compromise the security of other sites, tools used to collect email addresses for use in sending bulk email, or tools used to send bulk mail.

3.4 CUSTOMER receives a login and a password. CUSTOMER is responsible for changing its password when the account or Equipment is activated and have the password changed regularly. This password allows access to CUSTOMER account or Equipment and is used for several support and ordering services.

3.5 3W INFRA staff will ask for the login and a password in case of a support issue or emergency to authenticate CUSTOMER. CUSTOMER may sign a waiver to decline the use of a password and assume all risks, losses and liability that may arise by electing to receive these services without a remote access password. If there is no password or signed waiver from CUSTOMER, 3W INFRA staff will be unable to respond to CUSTOMER request.

3.6 CUSTOMER is responsible for the security of his or her Equipment password. Generally, secure passwords are between 6 and 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. CUSTOMER is responsible for changing his or her Equipment password regularly.

3.7 3W INFRA staff may monitor the security of CUSTOMER passwords at any time. A CUSTOMER with an insecure password may be directed to change the password to one that complies with the above rules. CUSTOMER who repeatedly chooses insecure passwords may be assigned a password by 3W INFRA.

4. SYSTEM SECURITY

4.1 CUSTOMER is prohibited from utilizing 3W INFRA's services to compromise the security or tamper with system resources or accounts on Equipment in 3W INFRA's Network or at any other site. Use or distribution of tools designed for compromising security is prohibited. Examples of these tools include but are not limited to password guessing programs, cracking tools or network probing tools.

4.2 3W INFRA reserves the right to release the contact information of CUSTOMERS involved in violations of system security to system administrators at other sites, in order to assist them in resolving security incidents. 3W INFRA will also fully cooperate with law enforcement authorities in investigating suspected lawbreakers.

5. EMAIL USE

5.1 3W INFRA will investigate complaints regarding email and may, in its sole discretion, take action based on the rules below. If an email message is found to violate one of the policies below, or to contain unlawful material, as described above, 3W INFRA may take action as outlined above.

5.2 CUSTOMER may not send email in any way that may be illegal. 3W INFRA recognizes that email is an informal medium; however, CUSTOMER must refrain from sending further email to a user after receiving a request to stop.

5.3 Unsolicited advertising mailings, whether commercial or informational, are strictly prohibited. CUSTOMER may send advertising material only to addresses that have specifically requested that material. Opt-Out mailings are prohibited.
5.4 CUSTOMER may not send, propagate, or reply to mail bombs. Mail bombing is defined as either emailing copies of a single message to many receivers, or sending large or multiple files or messages to a single receiver with malicious intent.
5.5 CUSTOMER may not alter the headers of email messages to conceal his email address or to prevent receivers from responding to messages.
5.6 Violations of the 3W INFRA policies outlined in this document can sometimes result in massive numbers of email responses. If a CUSTOMER receives so much email that 3W INFRA resources are affected, 3W INFRA staff may block access to CUSTOMER's equipment at the router and/or switch level.

6. WORLD WIDE WEB USE

6.1 3W INFRA will investigate complaints regarding inappropriate material on Web pages transmitted using 3W INFRA's services, in its sole discretion, require that the material be removed or take action as outlined above.
6.2 3W INFRA actively blocks the following ports for its entire network:

- UDP/1434 - SQL slammer/worm
- UDP/137 - Netbios
- UDP/139 – Netbios
- TCP/135 till 139 - Netbios
- TCP/445 - Smb
- TCP/593 - Rpc endpoint mapper
- TCP/4444 - Blaster/worm

7. IRC USE

7.1 CUSTOMER is prohibited from posting or transmitting inappropriate material via the use of IRC or to otherwise use IRC in a manner that is in breach of the Policies. For the purpose of this clause, prohibited is the use of IRC including so called 'eggdrop' and 'psybnc shell hosting'.
7.2 Without the prior written consent of 3W INFRA, CUSTOMER is prohibited from hosting an IRC server, regardless whether it concerns a stand-alone server or an IRC server that connects to global IRC networks.

8. ABUSE COMPLIANCE POLICY

8.1. ABUSE HANDLING REQUIREMENTS

8.1.1 In connection with the use of 3W INFRA's Services, CUSTOMER shall adopt and apply an abuse handling procedure which is compliant with the 3W INFRA Policies, with the law that applies to the Agreement and with any other law applicable to CUSTOMER.
8.1.2 CUSTOMER shall log each abuse notification received by CUSTOMER from 3W INFRA 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.

8.1.3 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.

8.1.4 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.

8.2. ABUSE HANDLING PROCEDURE

8.2.1 When 3W INFRA is notified by a third party of a (suspected) violation by CUSTOMER and/or the end-user of the Policies and/or applicable law, 3W INFRA shall notify CUSTOMER hereof by way of email or such other method of communication as 3W INFRA deems appropriate.

8.2.2 CUSTOMER shall, within the response period set forth in 3W INFRA's notification, take remedial action to cure the violation and within that period inform 3W INFRA of the action taken by CUSTOMER.

8.2.3 In some cases, 3W INFRA may grant the CUSTOMER the option to contest the alleged violation by filing a counter notice. If CUSTOMER chooses to file a counter notice, CUSTOMER must submit this in writing. 3W INFRA shall review the submitted information and may - in 3W INFRA's sole discretion – decide to reject CUSTOMER's counter notice, and require CUSTOMER to take immediate remedial action, if – in 3W INFRA's sole discretion – CUSTOMER or the end-user's content or actions are unmistakably unlawful and/or may subject 3W INFRA to third party claims and/or litigation.

8.2.4 If 3W INFRA does not reject CUSTOMER's counter notice, CUSTOMER shall – upon 3W INFRA's request – provide a deposit or a bank guarantee or other security satisfactory to 3W INFRA. The amount of security will be determined by 3W INFRA at its sole discretion. The security is intended to cover 3W INFRA's obligations, and any claim of 3W INFRA, under the indemnity specified in the Conditions. Furthermore, in the event that CUSTOMER files a counter notice, CUSTOMER shall within two (2) days of its response to 3W INFRA notify 3W INFRA whether an attorney will be representing CUSTOMER and, if so, which attorney.

8.2.5 CUSTOMER shall provide 3W INFRA with all documents and information in connection with the abuse notification without cost and on first demand.

8.2.6 As a condition to the (continued) provision of Services and/or to resuming the provision of Services, 3W INFRA 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(s).

8.2.7 In the event CUSTOMER is not able to comply with the abuse handling procedure, 3W INFRA may - in its sole discretion – decide to immediately discontinue - including (temporarily) disabling - the Services related to an abuse notification.

8.3. REPEAT INFRINGERS

8.3.1 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 service – (i) materials or date that violate or infringe the Policies; or (ii) that CUSTOMER previously deleted or disabled further to receipt of an abuse notification.

8.3.2 CUSTOMER shall immediately terminate the provision of service to an end-user – and terminate an end-user access to the Service – in the event that such end-user is discovered to be a repeated infringer or violator of the Policies.

8.3.3 In the event CUSTOMER's service 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.

8.3.4 In the event CUSTOMER is not able to provide an online tool, referred to in Clause 8.3.3, 3W INFRA may - in its sole discretion – decide to immediately discontinue - including (temporarily) disabling - the Services related to an abuse notification.

9. INVESTIGATION POLICY

9.1 3W INFRA reserves the right to conduct an investigation, based on (i) suspected violations of the Policies; and/or (ii) (potential) security risks to its Infrastructure (including but not limited to the Data Center and Network); and/or (iii) a valid request of the relevant (law enforcement) authorities.

9.2 As part of this investigation, 3W INFRA may, acting reasonably (i) gather information from or about CUSTOMER; (ii) if relevant, gather information from a complaining party. CUSTOMER is obliged to fully cooperate with any such investigations by 3W INFRA.

10. TERMINATION

10.1 If 3W INFRA terminates CUSTOMER's services during the Initial or Renewed Term due to a violation of the AUP by CUSTOMER, CUSTOMER shall pay to 3W INFRA, as liquidated damages and not as a penalty, an amount equal to the sum of (a) 100% (one hundred percent) of the total amount of Service Charges that would have become due during the period from the effective termination date to the expiration date of the Initial or Renewed Term, and (b) the amount of any Service Charges discounts granted to CUSTOMER by 3W INFRA in consideration of the length of the Initial Term (“Termination Charge”).

10.2 CUSTOMER shall pay the Termination Charge to 3W INFRA within five (5) business days of the termination date. CUSTOMER’s payment of the Termination Charge shall not prevent or limit 3W INFRA from pursuing any and all other available remedies against CUSTOMER. 3W INFRA reserves the right to hold any CUSTOMER Equipment until it has received the Termination Charge and disallow Data Center access of CUSTOMER. 3W INFRA reserves the right to sell any CUSTOMER Equipment in case CUSTOMER does not pay the Termination Charge within one (1) month after the termination date.