

## **SPECIAL CONDITIONS FOR SO YOU START DEDICATED SERVER RENTAL**

*Latest version dated 03/12/2013*

### **ARTICLE 1: PURPOSE**

The purpose of these Special Conditions, which supplement the So You Start General Conditions of Service, is to define the technical and financial conditions subject to which the Supplier will rent the Customer's So You Start dedicated server on its platform.

The Customer expressly recognises that under this Agreement, the Supplier does not participate, in any way whatsoever, in designing, developing, creating or setting up the Customer's website and their IT management and administration tools.

In the event of a conflict between these Special Conditions and the General Conditions of Service, these Special Conditions shall prevail.

### **ARTICLE 2: RESOURCES**

The So You Start server platform on which the Customer's dedicated server will be installed is accessible to the general public by way of stations connected to the internet.

Throughout the period of renting the dedicated server to the Customer, the Supplier shall provide the Customer with access to a forum, which the Customer may use to obtain technical advice.

### **ARTICLE 3: CONDITIONS OF SERVICE IMPLEMENTATION**

The Supplier will inform the Customer by email when their dedicated server has been made available. The point at which the dedicated server is put online shall determine the initial date on which invoicing will take effect.

The server will be made available after the Supplier has validated the initial payment and within a maximum period of 7 days from the date that the purchase order is paid by the Customer.

After this period and in the absence of provision of the server by the Supplier, the Customer reserves the right to request cancellation of the transaction and a refund of the sums already paid.

The server rented to the Customer shall remain the property of the Supplier. Any server rented from the Supplier will have a fixed IP address.

The technical specifications of the Service are detailed on the <https://www.soyoustart.ie> website.

The Customer is the administrator of the server rented from the Supplier. They may install software applications on the server themselves. In this instance, they shall assume full

responsibility for carrying out these installations, and the Supplier shall not be held liable for any malfunctioning of the server in relation to these installations.

#### **ARTICLE 4: SUPPLIER'S OBLIGATIONS**

The Supplier shall take all reasonable care and diligence necessary to provide a quality Service, conforming to the customary professional and state of the art practices. The Supplier undertakes to:

**4.1.** Use reasonable endeavours to maintain the Service in good working order. In the event of failure of the hardware rented to the Customer after creation of an incident ticket, the Supplier shall replace the defective part as soon as reasonably practicable. This provision shall not apply in relation to any failure for which the Supplier is not responsible, or any other intervention requiring an interruption or suspension of the Service for a period exceeding the usual replacement times. The Supplier shall inform the Customer immediately if the Supplier does not expect to be able to repair or replace the malfunction in the usual replacement times.

**4.2.** Guarantee the server's connection to the network via the internet 24 hours a day and every day of the year, unless otherwise stated in this Agreement. The Supplier reserves the right to stop the server's connection to the network in order to carry out a technical intervention on the devices of the Supplier network.

**4.3.** Intervene quickly in the event of an incident not involving misuse of the server by the Customer, on the Customer's intervention request.

**4.4.** Ensure that its resources comply with best quality standards at all times, in accordance with industry rules and practices.

#### **ARTICLE 5: SUPPLIER'S LIABILITY**

The Supplier reserves the right to stop the internet connection of the server rented to the Customer if this server poses a threat to the security maintenance of the Supplier platform whether resulting from hacking of the server, the detection of a security system loophole, or the need to update the server.

The Supplier shall inform the Customer as soon as reasonably possible if any maintenance, repair or upgrade requires the server to be suspended and of the likely duration of such suspension, so that the Customer may take appropriate measures. The Supplier shall inform the Client by email as soon as reasonably practicable if any maintenance, repair or upgrade requires the Dedicated Hosting Services to be suspended and shall inform the Customer of the likely duration of such suspension. The Supplier undertakes to restore the connection as soon as the corrective interventions have been carried out by the Customer.

In addition, the Supplier shall not be held liable for the content of the information, sound, text, images, shapes and forms and data accessible via the websites hosted on the Customer's server or transmitted or uploaded by the Customer in any respect whatsoever.

The Supplier shall have no liability to the Customer under this Agreement in the event of any interruption, partial or total failure due to any variation of the bandwidth or any failure of the Supplier's ISP/Access Provider.

## **ARTICLE 6: OBLIGATIONS AND LIABILITY OF THE CUSTOMER**

**6.1** The Customer is acting as an independent entity and, as such, accepts full responsibility for all risks and liabilities of their activity. The Customer is solely responsible for the services and internet websites hosted on the dedicated server, its content, use and the updating of information transmitted, distributed or collected and of all files, especially address files. The Customer specifically undertakes to respect the rights of any third parties, especially personality rights and intellectual property rights such as copyrights, design rights, patent rights or trade marks. The Supplier shall not be held liable for the content, usage or updating of any information or files, especially address files, whether transmitted, distributed or collected in any respect whatsoever.

The Supplier can only warn the Customer of the legal consequences that may arise from illicit activities on the server, and does not accept any responsibility regarding the use of the data made available to internet users by the Customer.

The Customer shall not undertake or attempt to undertake, any intrusive web activities whatsoever through the server, such as, without limitation, port scanning, sniffing and spoofing.

In such situations, the Customer will not be able to claim any reimbursement from the Supplier for amounts already paid.

**6.2** The Customer shall be solely liable for the consequences of any malfunctioning of the server resulting from any use by their personnel or any person to whom the Customer has supplied their password/s. Likewise, the Customer shall be solely liable for the consequences of losing the above mentioned password/s.

**6.3** In order to maintain the security level of the Customer's server and all servers present on its platform the Supplier undertakes to inform the Customer by email or via the Supplier Website of the availability of updates of the operating systems maintained by the Supplier, for which a security fault has been raised. If the update of these applications is not carried out according to the Supplier requests the Supplier reserves the right to stop the server's connection to the internet.

In the event of the Supplier detecting that the Customer's server has been hacked, an email will be sent to the Customer indicating that a reinstallation procedure is essential to maintaining the integrity of the server and the entire platform. The Customer may then carry out such a procedure via their management Interface after having made a backup of all of their data. The Supplier

reserves the right to stop the server's connection to the internet pending installation of the new machine. The Supplier is not obliged to carry out the transfer of data from the hacked server to the new server as this procedure is to be performed by the Customer themselves. The Supplier limits its intervention to installation of the new system only.

**6.4** For security reasons, the Supplier reserves the right to proceed with the immediate suspension without notice, of any server on which there is a public service Proxy, IRC, VPN or TOR which is available free of charge or for a fee, and for which the Supplier has knowledge of its fraudulent or illegal use.

**6.5** The Customer is responsible for taking all the necessary measures to back up their data.

**6.6** In the event that the Customer does not pay any licence or subscription fees when due to the Supplier or any third party, the Supplier reserves the right to suspend the Services without prior notice.

**6.7** The Supplier reserves the right to carry out checks and audits to ensure that the Customer's use of the Service is in compliance with these Special Conditions.

The Supplier reserves the right to suspend the Services without prior notice, and to terminate the server rental agreement:

- i) where the Customer's server poses a significant risk to the Supplier's infrastructure;
- ii) in the event of any non-compliance by the Customer with the Supplier's Special Conditions and/or General Conditions of Service; or in accordance with any applicable statutory and regulatory provisions, or pursuant to any contract it has with any third party.

**6.8** The Customer is reminded that any intervention by the Supplier of the Customer's dedicated server is limited to the installation of the server. For this reason, the Supplier only provides rental of the specialised infrastructure and does not assume any control over the contents of the websites hosted or the contractual relationship of the editors of these sites and their hosting provider, or the Customer under the dedicated server rental contract. In relation to the Customer's server, the Customer shall be a hosting provider and shall retain and preserve any data that will enable the identification of any third party who contributes to the content creation or to one of the contents of the services that he provides, for a period of 12 months, without engaging the liability of the Supplier in this respect.

The Customer shall implement an easily accessible and visible structure that enables any person to notify it of any offence or potential offence whatsoever that may have occurred on any website or contained in any data transmitted across the server network, including, but not limited to, data which constitutes incitement to racial hatred, child pornography, incitement to violence, violation of human dignity or illicit gambling activities. The Customer shall ensure that all required notices are set out on the website and that it is clear that the Customer is the hosting service provider in any legal notices presented by their contracting parties on their So You Start server.

## **ARTICLE 7: MEASURES FOR THE PREVENTION OF SPAMMING FROM THE SUPPLIER'S NETWORK**

The Supplier shall implement a system of technical measures intended to prevent the dispatch of fraudulent emails and spam from its infrastructure.

The Supplier shall monitor outgoing traffic from the Server towards port 25 (SMTP server) on the internet, which shall involve monitoring traffic by means of automatic tools.

The outgoing traffic shall not be filtered or intercepted but rather monitored by the Supplier with a delay of a few seconds. These operations shall be conducted by the Supplier in parallel between the server and the internet.

No operation is performed on sent emails. The Supplier shall not conduct any tagging of e-mails, and shall not modify e-mails sent by the Customer in anyway whatsoever. No information shall be stored by the Supplier during these operations aside from statistical data.

The operation shall be conducted regularly and in a fully-automated manner by the Supplier and the Customer acknowledges that no human intervention is involved during the monitoring of traffic to port 25 (SMTP port).

In the case of outgoing traffic from the Customer's server, including e-mails, being identified as spam or fraudulent e-mails, the Supplier shall inform the Customer by e-mail and block the Server's SMTP port.

The Supplier shall not keep any copy of e-mails sent from the Server's SMTP port, even when they are identified as spam.

The Customer must request unblocking of the SMTP port by the So You Start Technical Assistance.

Any new email identified as spam will entail a new blocking of the SMTP port by the Supplier for a longer period to be determined at the Supplier's reasonable discretion.

On the occurrence of the Supplier blocking the SMTP port for a third time, the Supplier reserves the right to deny any new request for the unblocking of the SMTP port.

## **ARTICLE 8: MITIGATION (PROTECTION AGAINST DOS AND DDOS ATTACKS)**

The Supplier shall implement protection against DOS (Denial of Service) and DDOS-type hacking attempts provided that these attacks are conducted in a manner reasonably considered to be serious enough by the Supplier to warrant such protection. In implementing such protection, the Supplier shall use reasonable endeavours to ensure that the operation of the Customer's Services is maintained throughout the duration of a DOS or DDOS attack.

This function involves monitoring the traffic sent to the Customer's Services from outside the Supplier's network. The traffic identified as illegitimate shall then be rejected by the Supplier prior to reaching the Customer's infrastructure, thus allowing legitimate users to access the applications offered by the Customer in spite of the attack.

The protection measures shall not apply in the case of attacks such as SQL injection, brute-force, abuse of security flaws or other types of attack that the Supplier considers are similar.

The Supplier shall take all reasonable care and diligence to protect the Service and the Customer acknowledges that the tools installed may not detect the attack and may not enable service operations to be maintained.

Due to the great complexity of the protection service the Supplier is only obliged to act to the extent it is possible that the tools installed detect the attack and enable service operations to be maintained.

Given the nature of a potential DOS or DDOS attack and their complexity, the Supplier shall implement different levels of traffic protection in an effort to preserve its infrastructure and the Services.

Once the attack is identified and mitigation is automatically activated, mitigation shall not be deactivated prior to the end of the 26-hour period. Therefore until the activation of the mitigation, the Service having to directly sustain the attack may lead its unavailability.

Once the computer attack has been identified and the mitigation has been automatically enabled, the mitigation cannot be disabled until the end of the 26 hour period.

While mitigation is activated, the Supplier shall not guarantee the accessibility of the Customer's applications but it shall endeavour to limit the impact of a DOS or DDOS attack on the Customer's Services and on the Supplier's infrastructure.

If, in spite of the activation of mitigation, a DOS or DDOS attack is of such a nature as to adversely affect the integrity of the Supplier's infrastructure or the infrastructure of the other customers of the Supplier, the Supplier shall strengthen its protection measures which may lead to the deterioration of the Customer's Services or impact its availability for which the Supplier shall not be liable.

Where part of the traffic generated by a DOS or DDOS attack is not detected by the Supplier's equipment and reaches the Customer's Services the effectiveness of the mitigation shall also depend on the appropriate configuration of the Customer's Services. In this regard, the Customer must ensure that it has the adequate resources to administer the configuration of the Customer's Services properly.

The Customer shall be solely responsible for ensuring they secure their Services, implementing security tools (firewall, etc.), periodically updating their system, backing up their data and for