

SPECIAL CONDITIONS FOR WEBSITE HOSTING SERVICES ON A DEDICATED SERVER

Version Date 03-09-13

The Supplier provides different categories of Dedicated Server. The hardware and software configurations, and the different tariffs applicable, are specified on the Supplier's website at www.ovh.co.uk.

1. INTERPRETATION

In these Special Conditions, the terms defined in the General Conditions shall have the same meanings and the following terms shall have the following meanings unless the context otherwise requires:

Content: the text, information, image, audio or video material and other data placed on the Dedicated Server by or on behalf of the Customer, including data which the Customer permits third parties to place on the Dedicated Server.

Customer: the person, firm or company who purchases Services from the Supplier.

Dedicated Hosting Services: the hosting of the Website on a Dedicated Server for the Customer's exclusive use.

Dedicated Server: the Supplier's server at www.ovh.ie on which the Website shall be hosted for the purpose of the Dedicated Hosting Services, and which shall have a fixed IP address assigned to it.

(D)DOS: (distributed) denial-of-service attack; an attempt to make a machine or network resource unavailable to its intended users.

General Conditions: the Supplier's general terms and conditions of services from time to time.

Internet Relay Chat (IRC): a protocol for live interactive internet text messaging

ISP/Access Provider: internet service provider/internet access provider.

PRO Option: the pro utilisation option of Services as specifically subscribed for by the Customer.

SMTP: simple mail transfer protocol; an internet standard for e-mail transmission across internet protocol networks.

SQL: structured query language; a special-purpose programming language designed for managing data.

Supplier: OVH Limited, a private company incorporated and registered in England and Wales under No 05519821, whose registered office is at Lincoln House, 300 High Holborn London WC1V 7JH, VAT No GB 918759474.

Website: the Customer's website(s) to be hosted on the Dedicated Server (including all data on such website(s) which is necessary for the publication and exchange of information via the internet).

2. APPLICATION OF THE CONDITIONS

These Special Conditions (together with the General Conditions) shall apply to any Contract between the Supplier and the Customer for the provision of Dedicated Hosting Services and shall prevail over any inconsistent terms or conditions submitted by the Customer or implied by law, trade custom, practice or course of dealing. In the event of conflict between these Special Conditions and the General Conditions, these Special Conditions shall prevail.

3. DEDICATED SERVER

3.1 The Dedicated Server shall remain the property of the Supplier at all times. The Customer shall not be entitled to sell, transfer, lease, charge, assign by way of security or otherwise deal in or encumber the Dedicated Server.

3.2 In order to maintain adequate security levels of the Dedicated Server and of all the servers hosted by the Supplier, the Supplier shall inform the Customer by email of the availability of Software upgrades for which a high level security failure has been noticed. The Supplier shall be entitled to disconnect the Dedicated Server if such upgrades are not carried out by the Customer following the Supplier's notification.

3.3 The provisions in the General Conditions relating to the provision of technical support shall not apply if the Customer has opted to use the Kimsufi support service.

4. SUPPLIER'S OBLIGATIONS

4.1 The Supplier shall provide the Dedicated Hosting Services with reasonable care and skill and in accordance with best industry practice.

4.2 The Supplier shall provide the Hardware and Software necessary for the provision of the Dedicated Hosting Services.

4.3 The Supplier warrants that the Hardware, Software and the Dedicated Server shall perform in accordance with the specifications set out in the Order.

4.4 The Supplier shall use its reasonable endeavours to ensure that:

the Hardware and Software is maintained in good working order and in accordance with best industry practice;

any defect, error or malfunction of the Hardware or Software is remedied as soon as is reasonably practicable, and the Customer is informed immediately if such repair or replacement requires the Dedicated Hosting Services to be suspended;

any disruption to the Dedicated Hosting Services which does not result from any breach by the Customer shall be rectified as soon as is reasonably practicable following a request from the Customer; and

subject to conditions 4.5 and 5 below, the Customer shall have access to the Dedicated Server via the Internet 24 hours a day, 365 days a year on the basis of the level of activity on the Website specified in the Order. If the level of activity on the Website exceeds that specified in the Order, the parties shall meet and agree an increased bandwidth usage and the corresponding additional fees.

4.5 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.

5. SUPPLIER'S LIABILITY

5.1 The Customer acknowledges that the Supplier shall not be responsible for any failure or malfunction of the Dedicated Server.

5.2 The Supplier shall have no liability to the Customer under the Contract in the event of:

any act, omission, fault or negligence of a third party not connected to the Supplier, and in particular any unauthorised access to the Website or the Content;

any act of piracy, viruses, worms, trojan horses or other harmful codes that affect or may affect the Dedicated Server, the Website and/or the provision of the Dedicated Hosting Services;

any actual or suspected security breaches in connection with the Dedicated Hosting Services;

any loss following the uploading of the Website to another server or IT system;

any modification (or attempted modification) of the Software by the Customer or a third party not authorised by the Supplier;

any loss caused by the operation or non-operation, use or non-use of the Website or the Content;

downtime caused by routine or emergency maintenance, repair or upgrade to the Dedicated Hosting Services provided that, if such maintenance, repair or upgrade requires the Dedicated Hosting Services to be restricted or suspended, the Supplier shall use reasonable endeavours to notify the Customer by email as soon as reasonably practicable in advance of the likely duration of such restriction or suspension and shall endeavour to resume the Dedicated Hosting Services as soon as reasonably practicable;

any interruption, partial or total failure of the Dedicated Hosting Services due to any variation of the bandwidth or any failure of the Supplier's ISP/Access Provider.

5.3 If the Supplier detects that the security or integrity of the Website has been compromised, the Supplier shall inform the Customer by email that the Content must be re-installed, and the Supplier shall be entitled to protect the integrity of the Dedicated Server by disconnecting it from the internet until the Website has been reinstated. The Customer shall be responsible for reinstalling the Content. The Supplier's sole responsibility shall be to reconnect the Website to the internet once it has been reinstated.

5.4 In so far as the Supplier is susceptible to receiving notifications of illicit use of an internet protocol address ("IP Address") attributed to a Customer, said Customer will be assessed according to the law applicable to the location of the Customer and the Supplier can offer the Customer an IP address corresponding to the state/country to which they are established and/or to which the Customer must move their service.

5.5 The Customer is therefore required, when using an IP address corresponding to a particular state/country, to comply with all laws and regulations of that state/country. In the case where the Supplier receives notification stating the violation by the Customer of the applicable law of the state/country for their corresponding IP address, the Customer must take all necessary measures to cease the violation in question. Otherwise, the Supplier reserves the right to suspend service.

6. CUSTOMER'S OBLIGATIONS

6.1 The Customer shall be solely responsible for:

uploading the Content onto the Server and checking that it functions satisfactorily. The Supplier shall not be responsible for any failure of the Customer to upload the Content correctly, and shall not be responsible for providing support in relation to the control and operation of the Content;

the Content, for the conception or development of the Website, and for the Customer's equipment, systems or software necessary for the management of the Website. The Supplier shall have no obligation to validate or vet the Content for usability, legality, content or correctness and shall not, in any event, be liable towards the Customer or any third party for any loss arising from or in connection with the Content;

complying with all applicable laws and regulations concerning the Content, including (without limitation) for ensuring that the Website contains all information concerning the Customer, its products and the conduct of its business which are required;

ensuring that the Content, any material linked to the Website and any activity conducted via the Website do not breach the rights of any third parties including without limitation any intellectual property rights; and

making regular back ups of the Content on any website from time to time.

6.2 The Customer shall use its best endeavours to ensure that all Content on the Website does not contain any viruses and/or other harmful code.

6.3 The Customer shall be solely liable in respect of any and all data it makes available to web users. The Supplier shall not be liable for any losses, claims or damages (howsoever arising, including negligence) in relation to such data.

6.4 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.

6.5 In the event that the Customer is in breach of either clauses 6.3 or 6.4, it shall not be entitled to claim any refund from the Supplier of amounts already paid.

6.6 The Customer shall be solely responsible for any Server malfunction arising from any use by any other person to whom the Customer may have provided its password(s). The Customer shall also be solely responsible for any loss of the abovementioned password(s).

6.7 In order to preserve the existing level of security of the Customer's server and of all servers forming part of its platform, the Supplier undertakes to notify the Customer, by e-mail through the dadies@ml.OVH.net mailing list, of the availability of updates for applications maintained by the Supplier, for which a security issue is observed. If the update of these applications is not performed by the Customer promptly following the Supplier's notification, the Supplier reserves the right to suspend the Server's connection to the internet.

6.8 Where the Supplier detects that the Customer's computer has been hacked or a similar event has occurred, an e-mail will be sent to the Customer within a reasonable period of time, informing it that re-installation is necessary to maintain the integrity of the Server and of all servers on the platform. The Customer may then carry out such re-installation through its management interface, after having backed up all its data. The Supplier reserves the right to suspend the Server's connection to the internet pending the Customer's full and complete re-installation of the computer. The Customer is solely responsible for transferring the data from the hacked system to the new one and the Supplier's sole responsibility is to install the new system.

6.9 For security reasons, OVH 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 OVH has knowledge of its fraudulent or illegal misuse.

6.10 The Customer is responsible for taking all measures necessary to back up its data.

6.11 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.

6.12 The Supplier reserves the right to audit the Customer's compliance with the Services and with the provisions contained in these Special Conditions and the General Conditions at any point during the term of these Special Conditions with 5 Working Days' prior written notice to the Customer. The Supplier may have access to and take copies of the Customer's records and any other information held at the Customer's

premises and to meet with the Customer's personnel to audit the Customer's compliance with its obligations under these Special Conditions and the General Conditions. Such audit rights shall continue for three years after termination of these Special Conditions. The Customer shall give all necessary assistance to the conduct of such audits during the term of these Special Conditions and for a period of three years after termination of these Special Conditions.

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

i) where the Customer's Server poses a significant risk to the Supplier's infrastructure; and

ii) in the event of any non-compliance by the Customer with the Supplier's special and standard terms and conditions; and in accordance with any applicable statutory and regulatory provisions, and pursuant to any contract it has with any third party.

6.14 The Supplier's obligation in relation to private servers is limited to the installation of the server and the opportunity for the Customer to rent the infrastructure. The Supplier has no control over the content of data held on the hosted websites. The Customer shall hold and preserve, for a period of 12 months from its creation, all data ("**Web Data**") that would enable the identification of any party that has contributed in anyway whatsoever to the creation of any content contained on any hosted website that may be accessed via the Server. The Customer shall be solely responsible and liable in respect of the holding and preserving of all Web Data.

6.15 Further to clause 6.14, 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, as well as 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 its contracting parties editing a website.

7. Measures for the prevention of spamming from the Supplier's network

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

7.2 Further to 7.1, 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.

7.3 The outgoing traffic referred to in 7.2 shall be monitored by the Supplier with a delay of a few seconds, rather than being filtered or intercepted. These operations shall be conducted by the Supplier in parallel between the Server and the internet.

7.4 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.

7.5 The operation in 7.4 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).

7.6 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.

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

7.8 The Customer may request unblocking of the SMTP port through its management interface.

7.9 Any new e-mail 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.

7.10 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.

8. Mitigation (protection against DOS and DDOS attacks)

8.1 The Supplier shall implement protection against DOS 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.

8.2 The function in clause 8.1 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.

8.3 The protection measures outlined in clauses 8.1 and 8.2 shall not apply in the case of attacks such as SQL injection, brute-force, abuse of security flaws or in similar-type attacks.

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

8.5 Mitigation of a DOS or DDOS attack is only activated on detection of the attack by the Supplier's tools and for a minimum period of 26 hours. Until activation of the mitigation, the Services shall bear the attack directly, which may lead to the temporary unavailability of the Services.

8.6 Once the attack is identified and mitigation is automatically activated, mitigation shall not be deactivated prior to the end of the 26-hour period.

8.7 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.

8.8 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.

8.9 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.

8.10 The Customer shall be solely responsible for ensuring it secures its Services, implementing security tools (firewall, etc.), periodically updating its system, backing up its data and for ensuring the security of its software (scripts, codes etc.).

Mitigation with the PRO Option:

If the Customer has subscribed for the PRO Option, new functions are available:

a) The Customer may trigger early activation of mitigation on its Services, although the Customer acknowledges and accepts that activation of mitigation may directly impact the quality of its Services and that the Supplier accepts no responsibility for this.

b) The Customer may, whenever it so wishes, test the various protection profiles in order to measure the impact on its Services and consequently identify the protection profile that is best suited to the type of Services found on its Server. The profile chosen by the Customer will then be automatically used by the Supplier upon activation of mitigation.

c) The Customer may also subscribe for a firewall that will directly operate on the boundary of the Supplier's network. When the mitigation is activated on the Customer's Services, firewall rules shall be automatically applied. The Customer shall be solely responsible for ensuring that the rules it incorporates in its firewall are such that they do not downgrade its activity on activation of mitigation.

9. Kimsufi 2013 range

9.1 The Kimsufi 2013 range is only available for individuals or legal entities domiciled in the European Union, Norway or Switzerland. The Customer may not have more than three Kimsufi 2013 servers simultaneously.

9.2 The Kimsufi 2013 server range is strictly reserved for personal use; any subscription to this range for re-sale purposes is prohibited and shall entail immediate termination of the rental agreement for the relevant Server(s).

9.3 As part of the Kimsufi offer, the Customer is informed that instead of the technical support as may be described with the General Conditions, it shall only be able to use the support forum accessible at: <http://forum.ovh.co.uk>.

10. Term and Termination

10.1 Notwithstanding condition 11.1 of the General Conditions, the Supplier shall send the Customer at least 6 reminders on the following dates:

1st reminder 60 days before Expiry Date;

2nd reminder 30 days before Expiry Date;

3rd reminder 15 days before Expiry Date;

4th reminder 7 days before Expiry Date;

5th reminder 3 days before Expiry Date.

10.2 The Supplier shall be entitled to terminate the Dedicated Hosting Services for its own convenience at any time and without incurring any liability by giving 30 days' written notice to the Customer.

10.3 The Supplier shall be entitled to suspend the Dedicated Hosting Services without incurring any liability if the Customer commits a breach of condition 6 of these Special Conditions and, for the purpose of condition 11.5(a) of the General Conditions, any breach of condition 6 of these Special Conditions shall be deemed to be a material breach of the Contract.

10.4 The Supplier shall be entitled to disconnect the Dedicated Server and/or to erase the Content and any material uploaded on the Dedicated Server 5 days after the Expiry Date or forthwith upon the termination of the Contract for any other reason whatsoever without incurring any liability towards the Customer.