



SPECIFIC TERMS AND CONDITIONS ON THE RENTAL OF A KS (KIMSUFU) DEDICATED SERVER

Latest Version on September 2nd 2014

SECTION 1: PURPOSE

The purpose of these Specific Terms and Conditions, which are complementary to KIMSUFU's General Terms and Conditions of Service, is to define the technical and financial terms and conditions pursuant to which OVH agrees to rent and host on its platform the Customer's KS (KIMSUFU) dedicated internet server.

The Customer hereby recognizes expressly that OVH shall not participate in any way in the design, development, realization and set-up of the Customer's website and/or services and of its management and administrative computer tools within the meaning of this agreement.

In the event of a conflict between the General Terms and Conditions and these Specific Terms and Conditions, the latter shall prevail.

SECTION 2: MEANS

The KIMSUFU platform server, where the Customer's dedicated server will be installed shall be accessible to the public on the internet network via stations connected to the network.

SECTION 3: TECHNICAL SUPPORT

Technical assistance is made available to the Customer solely by a forum hosted at <https://forum.ovh.ca/>.

The customer is responsible for mentioning any problem on this forum.

SECTION 4: DELIVERY OF SERVICE TERMS AND CONDITIONS

OVH shall inform the Customer by e-mail when the dedicated server becomes available. Invoicing shall begin on the effective date of the online launching of the dedicated server.

The server shall become available within a maximum of 7 days of the effective payment date by the Customer of the purchase order.

After such deadline has expired and if OVH fails to make available the server to the Customer, said Customer shall be entitled to request the cancellation of the transaction and the reimbursement of amounts already paid.

The server rented to the Customer shall remain the property of OVH. Any server rented or hosted by OVH has a static IP address. The server shall be hosted on OVH's server platform.





The Customer is the administrator of the server rented from OVH. He/It may install on his/its own the software applications on the server. He/It is fully responsible for the software installation, and OVH may not be held liable for any server malfunction following such installation.

SECTION 5: OVH'S OBLIGATIONS

OVH agrees to use all due care and due dispatch to provide a quality service in compliance with professional standards and the state of the art. OVH agrees to:

- 5.1. Keep the material in good working condition. In the event of failure of the material rented out to the Customer, OVH agrees to replace any defective parts at its earliest convenience, except in cases where it is not liable for the failure, or of any other intervention which would require an interruption of service beyond the usual replacement wait times. In the latter case, OVH shall immediately notify the Customer.
- 5.2. Ensure access to the server via internet 24 hours a day, every day of the year. OVH reserves the right to interrupt the server for a technical intervention designed to improve its operation.
- 5.3. At the customer's request intervene quickly in the event of a malfunction not resulting from a misuse of the server by the Customer.
- 5.4. Ensure that its tools are maintained at the highest quality level in compliance with professional rules and standards.

SECTION 6: OVH'S LIABILITIES

OVH reserves the right to interrupt the rented server's internet connection if such server constitutes a danger regarding the maintenance of security on OVH's hosting platform, whether this is as a result of the piracy of such server, the detection of a flaw in the security system, or the need to update the server.

OVH shall, to the extent possible, notify the Customer in advance and within a reasonable deadline, by informing him/it of the nature and the length of the intervention, in order to enable such Customer to make arrangements in that regard. OVH shall restore the connection as soon as the corrective measures have been completed.

OVH shall not be liable for the content of information, sound, text, images, elements of form, or data accessible on the websites hosted on the Customer's server, which are transmitted or placed online by the Customer for any reason whatsoever.

OVH shall not be liable in case of a violation, in whole or in part, of an obligation or of a network operators' flaw in transmission to the internet, especially if it involves its access provider(s).

LIMITED LIABILITY

THE CUSTOMER ACKNOWLEDGES THAT OVH AUTHORIZES OTHER SERVICE USERS TO INSTALL THEIR WEBSITES AND SERVERS IN ITS FACILITIES. OVH SHALL NOT BE LIABLE IN ANY WAY WHATSOEVER FOR DAMAGES, COSTS OR LOSSES INCURRED BY THE CUSTOMER (OR BY THE LATTER'S OWN CUSTOMERS) AND CAUSED BY ANOTHER SERVICE USER'S ACT, MATERIAL OR FAILURE TO ACT. OVH'S LIABILITY IN CONTRACT, IN





TORT (INCLUDING NEGLIGENCE) BY STATUTE, OR OTHERWISE, TO THE CUSTOMER (OR THE LATTER'S OWN CUSTOMERS), CONCERNING PERFORMANCE OR NON-PERFORMANCE, AS APPLICABLE, OF ANY OBLIGATION CREATED UNDER THIS AGREEMENT, WITH REGARD TO ANY CLAIM, SHALL BE LIMITED AND SHALL NOT, IN THE AGGREGATE, EXCEED THE TOTAL FEES PAID BY THE CUSTOMER TO OVH UNDER THIS AGREEMENT IN THE THREE- (3-) MONTH PERIOD IMMEDIATELY PRECEDING THE DATE ON WHICH THE CLAIM AROSE. IN NO EVENT SHALL OVH BE LIABLE FOR ANY LOST PROFITS, OR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES.

SECTION 7: CUSTOMER'S OBLIGATIONS AND LIABILITIES

7.1 The Customer acts as an independent entity and therefore assumes all the risks related to his/its activities. The Customer is solely liable with regard to the use of the services and websites hosted on his/its dedicated server, the content of the information transmitted, posted or collected, including operations and updates, as well as with regard to all files, including address files. The Customer agrees, more specifically, to comply with the rights of third parties, human rights, and intellectual property rights, such as copyrights, patent rights or trademarks. OVH shall therefore not be liable, in any way whatsoever, for the content of information transmitted, posted or collected, used, and updated, as well as for any files, including address files.

OVH alerts the Customer as to the legal consequences that could result from unlawful activities on the server, and disclaims any joint and several liabilities regarding the use of the data made available by the Customer to internet users.

The Customer shall also refrain from any breach or attempted breach activities (such as port scanning, sniffing, spoofing, etc.) while using the server.

In such cases, the Customer shall not be entitled to the reimbursement by OVH of amounts already paid in.

7.2 The Customer alone shall bear the consequences of a server malfunction resulting from the use by his/its staff or by any other person to whom the Customer has provided his/its password(s). The Customer shall also bear alone the consequences resulting from the loss of such password(s).

7.3 In order to maintain the security level of the Customer's server, and of all its servers on its hosting platform, OVH agrees to notify the Customer (via the forum) of the availability of updates for its applications where security flaws have been reported. If these application updates are not carried out at OVH's request, OVH reserves the right to interrupt the server's connection to the internet network.

Similarly, in the event OVH detects that a Customer's computer is subject to piracy, an e-mail shall be sent to such Customer, advising him/it that he/it should use a reinstallation procedure in order to ensure the integrity of his/its server and of the entire hosting platform. The Customer may order such procedure from OVH after backing up all his/its data. While awaiting the computer's reinstallation, OVH reserves the right to interrupt the server's connection to the internet network. OVH is not required to transfer the data from the pirated system to the new system; such operation is the Customer's responsibility. OVH hereby agrees to limit its intervention to the installation of the new system.

7.4 For security reasons, OVH can proceed with the immediate suspension (without notice) of any server on which would be offered paid or free public proxies, such as IRC, VPN, TOR for which OVH have knowledge of misuse, fraudulent or unlawful use.





7.5 The Customer shall take all required measures to ensure the backup of his/its data.

7.6 The Customer shall pay for any license or right to use he/it has agreed to with OVH, or with a third party, failing which, OVH reserves the right to suspend the service without prior notice.

7.7 OVH reserves the right to check the Customer's compliance with the provisions regarding use of the service.

OVH reserves the right to suspend the service without prior notice, as provided under section 7 of KIMSUF1's general service terms and conditions, in the event the Customer fails to comply with KIMSUF1's specific and general terms and conditions of service and, generally, with all laws and regulations in force, as well as with rights of third parties.

7.8 The Customer is reminded that OVH's intervention in connection with the contract on a dedicated server is limited to installing the server. OVH only insures in that regard the rental of a specialized infrastructure, without any control whatsoever over the content of the hosted websites or the contractual relationship between the sites' editor and their Web host, an OVH Customer under a dedicated server rental contract. The Customer shall therefore be considered a Web host.

7.9 The Customer acknowledges and agrees to be also subject to the laws applicable in the territory on which the equipment are installed. Hence, the Customer acknowledges OVH's right to suspend his service if it is used for a prohibited activity at the place of physical location of the equipment provided by OVH. The Customer also agrees that the same right applies on IP addresses and the Customer acknowledges OVH's right to suspend an IP if it is used for a prohibited activity at the place of registration of the IP. In the event of such use, OVH may suspend all the IP address of the Customer registered in the same location.

SECTION 8 : MEASURES AGAINST SPAM SENDING FROM OVH NETWORK

OVH is implementing a set of technical measures to fight against the sending for fraudulent e-mails as well of SPAM from its infrastructures.

To this end, OVH performs some verification on the traffic sent from the server used by the client to port 25 (SMTP) on the Internet. The traffic is analyzed by automatic tools .

Emails sending are neither filtered nor intercepted but checked with a time lag of a few seconds. These operations are performed in parallel and in sequentially before the emails are sent to the Internet.

Similarly, no operation is performed on the emails sent: OVH does not tag emails, and does not alter in any way the emails sent by the Client. No information is stored by OVH during these operations outside of statistics.

This operation is done regularly and is fully automatic. No human intervention is performed when checking traffic to port 25 (SMTP port).

In the case of the emails sent from a Client's server identified as spam or fraudulent, OVH will inform the Client by email and will block the SMTP server port.

OVH does not retain any copies of emails sent from the SMTP Server even when identified as spam.

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





Any new email identified as spam will result in a new blocking of the SMTP port for a longer time.

From the third blocking, OVH reserves the right to refuse any request to unblock the SMTP port.

SECTION 9: MITIGATION (PROTECTION FROM DOS AND DDOS ATTACKS)

OVH is implementing a protection against Denial Of Service (DOS) and Distributed Denial Of Service (DDOS) computer attacks and provided when made in a massive way. This feature is intended to prevent the Customer's operations to be inaccessible during the attack.

This object of this feature is to check the traffic to the Customer's Service and from outside of the OVH network. The illegitimate qualified traffic is then rejected upstream in the Client's infrastructure, allowing legitimate users to access the Service despite the undergoing cyberattack.

These safeguards do not prevent other computer attacks such as SQL injection, bruteforce, security vulnerabilities' exploitation etc.

Due to the great complexity of this Protection Service, OVH is not subject to an obligation of means; it is possible that the attack is not detected by the tools in place, and that the tools developed do not prevent the operation of the Service to be interrupted.

Depending on the nature of the attack and its complexity, OVH deploy a protection at different levels of traffic to preserve its infrastructure and the Customer Service.

Mitigation is activated only after the attack is detected by OVH tools, and a minimum of 26 hours. Therefore until the activation of mitigation, the Service is frontally affected by the attack, which can lead to its unavailability.

As soon as the cyber attack is identified and mitigation is automatically activated, mitigation can not be disabled until the end of a 26 hours period.

Throughout the duration of the activation of mitigation, OVH can not guarantee the availability and accessibility of the Client's applications but will try to limit the impact of this attack on Customer's Service and on OVH's Infrastructure.

If, despite the activation of mitigation, the cyber attack is likely to jeopardize the integrity of the OVH's or of other OVH customers, OVH will strengthen its protective measures which may cause a degradation of the Customer Service or impact its availability.

Finally, it is possible that some of the data generated by the attack can not be detected by the OVH equipment and reach the Customer Service. The effectiveness of mitigation also depends on the configuration of the Customer's Service; as such, it is up to them to verify that they have the necessary skills to ensure proper administration.

The mitigation does not exempt the Client to secure its Service, to implement security tools (firewalls ...), to regularly update its system, backup its data or to ensure the security of its computer programs (scripts, codes ...).

