VSCALE. Service Level Agreement

Terms and Abbreviations

Customer's Control Panel – the web page intended for managing the Services rendered by the Executor, retaining the Customer's actual contact information and providing other information necessary for the Executor to render Services to the Customer. Customer's Control Panel is available at the URL https://vscale.io/panel/. Access to the web page is arranged via secured protocol and only after the Customer has been identified.
Ticket System – the messaging system between the Customer and the Executor by means of sending/receiving requests electronically, located in the Customer's Control Panel.
Profile – Information intended for identifying the Customer during the process of rendering the Services. Profile information consists of the Customer's user name (login), password to access the Customer's Control Panel (password), and the Customer's agreement number.
Customer's Personal Account – the Customer's financial account with the Executor. The Customer may add funds to the Customer's Personal Account in order to pay for services rendered by the Executor.
Service Balance – the Customer's financial account with the Executor used for paying for the Vscale service. The Customer transfers funds from the Customer's Personal Account to the Customer's Service Balance in order to pay for services rendered by the Executor.
Customer's Bonus Balance – the Customer's financial account with the Executor used for paying for the Vscale service. The Executor adds funds to the Bonus Balance within the framework of promotional offers and in the form of compensation for a violation of the Service Level Agreement. When paying for services, funds shall first be taken from the Bonus Balance and then from the Storage Balance.
Virtual Machine – a virtual server, created in the Executor's Data Center, whose computational resources are made available to the Customer.
Backup – a copy of a file or other item of data made in case the original is lost or damaged.
API – a software interface used for automating service management.
SPAM – unsolicited bulk messages sent via electronic messaging systems (including e-mail, ICQ, etc.).
OS – The computer operating system.
IP address – An address assigned to an Internet connection
UDP amplification - a denial-of-service attack that operates on UDP.
Contract – the signed bilateral agreement or accepted offer between the Executor and Customer containing the terms which govern the actions of the Executor and Customer while rendering and using services, not excluding the Vscale service.
SLA – the present agreement (henceforth the Agreement) which regulates the procedure for rendering the Virtual Private Cloud service. The Agreement is considered an integral part of the Contract.

1. Service Description

1.1. The Executor shall render IT services in the form of creating a virtual server, making its resources (Executor's limited server resources) available to the Customer, and providing data backups of said servers. Customer is obliged to pay for these services according to the terms indicated in the Contract and present Agreement.

2. Ordering and the Provision of Services

2.1. Services can be selected and ordered directly by the Customer, without the involvement of the Executor, from the Customer's Control Panel.
2.2. The Services commence the moment they are made available by the Executor, provided the Vscale Service Balance has enough funds to pay for the Services.

3. Terms of Rendering Services

3.1. Equipment installation

3.1.1. Using the tools available in the Control Panel, Customer shall order a virtual server by choosing and entering the parameters for the required resources: an operating system from the list of those available in the system, a server configuration corresponding to a set payment plan, the geographic location of the server (St. Petersburg or Moscow), and others. Servers are set up automatically.
3.1.2. To order the backup service, Customer must choose the virtual server a backup should be made of. Backups are created automatically.

3.1.3. Hourly service costs are charged according to the costs listed on the Executor's site and Customer's Control Panel. Funds are removed from the Service Balance once an hour. Costs are set per hour and per month. If the virtual machine runs for more than 672 hours a month, the cost for the month shall not change.

3.1.4. The Customer may change his payment plan on his own, without the involvement of the Executor. If the plan is changed, the Customer is charged the maximum price for the hour the change took place. In this case, the payment plan may only be replaced by a more expensive plan. The hour count shall restart within a month of changing the server configuration.

3.1.5. The payment plan for the ordered and rendered services cannot be substituted for a less expensive option. If the Customer intends to choose a plan with a lower service cost and plans on discontinuing the use of previously ordered and rendered services, the service must be reordered and the necessary parameters and cost must be selected. In this case, the previously ordered service and corresponding data will be deleted.

3.1.6. A server that is turned off shall be charged according to the process outlined in section 3.1.3. Funds shall cease to be removed the hour following the hour when said server is deleted.

3.1.7. The maximum bandwidth of each virtual machine is 1000 Mbps depending on network utilization.

3.1.8. Traffic is not limited in terms of volume; however, Executor reserves the right to block any virtual machine and/or establish monthly traffic limits if any potentially harmful actions are detected. Limits from 1TB to 5TB may be set for each virtual machine depending on the applicable payment plan.

3.1.9. To prevent distributed denial-of-service (DDoS) attacks, the total bandwidth for UDP traffic shall be limited to 50 Mbps on ports 0, 16, 19, 53, 123, 520, and 1900.

3.1.10. To prevent denial-of-service attacks, the Executor has the right to limit bandwidth to 100 Mbps when the Customer exceeds the threshold of 150 000 packets per second.

3.1.11. To prevent denial of service attacks, the Executor has the right to limit the bandwidth of the Customer's services which may be exploited in UDP amplification attacks.

3.1.12. To prevent distributed denial-of-service (DDoS) attacks, incoming and outgoing UDP traffic on ports 17, 111, 520, 1900, and 11211 has been blocked at the edge router level. UDP traffic is transferred in its entirety within Executor's network infrastructure (including Internet and local network ports).

3.2. Service usage

3.2.1. The Customer shall operate virtual servers remotely via a general network connection or the Control Panel and install and set up necessary software on the virtual machines directly, without the involvement of the Executor.

3.2.2. Customer or an entity authorized by Customer may create or delete virtual servers and/or backups from the Control Panel at any time.

3.2.3. Customer can manage created servers from the Control Panel or via API, the documentation for which can be found at https://developers.vscale.io/documentation/api/v1/.

3.2.4. In the event the Customer uses equipment to perform an activity which, according to Russian law, should be licensed and certified, the Customer must have relevant licenses, certificates and other approvals necessary to perform the aforementioned activities on the territory of the Russian Federation. The Executor has the right to require the Customer to provide copies of the aforementioned documents.

3.3. Suspension and termination of services

3.3.1. When the funds in the Service Balance reach zero or are insufficient to pay for the following hour of service, there are no longer funds in the Service Balance (a balance of zero), the Service shall be suspended automatically. The Executor shall send the Customer notification of the suspension of the Service via Ticket System and/or email.

3.3.2. In the event of a 0 Service Balance or insufficient balance, as indicated in section 3.3.1, for a period 168 hours, the Executor has the right to delete all of the Customer's virtual servers and their backups saved on the Executor's equipment.

3.3.3. Customer may continue to use the Services by adding the necessary funds to the Balance within 168 hours after the Services have been suspended. Billing shall continue to apply to existing servers and backups for the entirety of the suspended period. If the Service is extended (funds are added to the balance) within the indicated or otherwise agreed upon period of time, and if there is an outstanding debt for previously used resources, the funds added to the balance will immediately be used to pay off the outstanding debt.

3.3.4. In the event the Customer terminates the Services, expressed as the complete deletion thereof and full payment as per section 3.1.6, all remaining funds on Customer's Personal Account are subject to refund.

3.3.5. The Service may be suspended if the Customer violates the present legislation or terms of the Contract or Agreement, or as the result of planned maintenance performed by the Executor. Planned maintenance occurs no more than 5 hours per quarter and on 1 (one) virtual machine. The Executor shall inform the Customer via Ticket System and/or email and/or by posting notification in the Control Panel of the planned maintenance no later than 3 (three) business days before the service suspended.

4. Requirements for protecting information

4.1. The Customer shall guarantee the security and actuality of the software used on his equipment and perform timely updates or change configurations of the software in accordance with the instructions and requirements published by the software developers and/or Internet security services.

4.2. The Customer shall take reasonable efforts to prevent any incidents of unauthorized access to the software and equipment used and not allow his own resources or those provided by the Executor to be used for attempts of unauthorized access to other Internet resources. In particular, the Customer should not allow the following to occur on/from his equipment:

- the sending of email messages from addresses not on the Customer's domain;
- the use of default passwords on the server's software;
- the sending of packets from a falsified IP source address;
- the sending of DNS packets with intentionally corrupt data;
- the presence of malware;
- the presence or use of software designed for granting unauthorized access to information on the server.

4.3. In order to verify compliance with the security requirements, the Executor shall reserve the right to periodically scan the Customer's services and servers using special software, provided it shall not harm the Customer's equipment or the information contained therein. The Executor shall inform the Customer of any violations detected during such inspections, and the Customer shall take necessary measures to eliminate them.

4.4. In the event a gross violation of information security, which may endanger the functioning of resources on another local or global computer network (which is not owned by the Customer), is detected, the Executor has the right to block the Customer's use of the equipment, the Services, or the resources which violate the security requirements.

4.5. The Executor, reserving all rights hereunder, can immediately suspend the Services in the following cases:

- if, in the justifiable opinion of the Executor, the Customer's use of the Services may harm the Executor and/or cause failure in the hardware and/or software of the Executor or third parties;
- the detection of Customer actions or intentions of sending, publishing, transferring, reproducing, distributing by any means, or using software and/or other materials, received in any form during the use of the Services, fully or in part, protected by copyright or other rights, without the consent of the rights holder;
- the detection of Customer actions or intentions of sending, publishing, transferring, or distributing by any means any information or software which contains viruses or other harmful components;
- the detection of Customer actions or intentions of sending Spam without the consent of the addressee, provided there is a written statement from the Spam receivers to the Executor containing justified claims against the Customer. In this case, "Spam" is defined on the basis of common "network use rules" published on the Internet and being customary business practice;
- the distribution and/or publication of any information which contradicts the effective Russian legislation, the provisions of the licenses of the Ministry of Communication of the Russian Federation (the Ministry of Information Technologies and Communications of the Russian Federation), or international regulations or infringes on the rights of third parties;
- the publication or distribution by the Customer of any data or computer software which contains code which acts similarly to computer viruses or other similar components;
- the advertising of services, products, or other materials which are limited or prohibited by the effective legislation;
- the falsification of an IP address (henceforth IP spoofing) or addresses used in other network protocols when transferring data over the Internet;
- using a falsified IP address or other network protocol addresses when transferring data to the Internet.
- the use of nonexistent return addresses when sending electronic messages;
- if actions are taken to disrupt the standard functions of Internet components (computers, other equipment, or software) not owned by the Customer;
- if actions are taken to obtain unsanctioned access to network resources (computers, other equipment, and information resources), the subsequent use of such access, or actions are taken to destroy or modify software or data not owned by the Customer without the consent of the owners of such software or data or the administrators of this information. Unsanctioned access is deemed to be any method other than that which is used by the owner of the resource;
- if actions are taken to transfer senseless and useless information to the computers or equipment of third parties or intermediate sections of the network in volumes exceeding the minimum permissible for inspecting the connectivity and accessibility of its separate components, effectively creating an excessive (parasitic) load for these computers or this equipment;
- if actions are taken to scan Internet sites in order to reveal the underlying structure of the sites, vulnerabilities, lists of open ports, etc. without the expressed consent of the owner of the inspected site;
- if other actions, which are not specified in the Contract and/or Agreement but contain criminal components or violate the rights and legal interests of third parties, are taken;
- in the event the Executor receives relevant instruction from the government body regulating such situations and has relevant powers in accordance with the effective Russian legislation.

4.6. The Executor shall not be liable for the content of data created and maintained by the Customer or users and shall not perform any preliminary censorship. If any gross violation of legislation takes place, the Services may be suspended

without prior notification. In this case, the Executor has the right to control the contents of the information resources of the Customer and users thereof.

4.7. The Executor shall not be liable for any violation of the rights of third parties resulting from the Customer's actions during the use of the Services provided by the Executor.

4.8. The period of suspension of the Services for reasons indicated in par. 3.3.5. shall not be considered an interruption of the Services and thus shall not be considered the failure of the Executor to fulfill the obligations stipulated in the Contract and present Agreement.

4.9. The Customer shall be fully liable for the compliance of the contents of his server (on site) and the actual location of this information (distributed or transferred) with the effective legislation.

4.10. The Customer shall be fully responsible for the risks related to the use of the Internet via the Executor's resources and/or the Services.

4.11. Executor's resources may not be used for organizing or performing actions to create new blocks for ensure the functionality of cryptocurrency platforms (mining).

5. Guarantee and Compensation

Availability*	24x7x365 - 24 hours a day, 7 days a week, 365 days a year
% (percent) of operability per month*	99.98%

Table 1. Unavailability of Customer's virtual machines as the result of failures in the infrastructure within the Executor's area of responsibility.

Availability of service	Unavailability per month	Compensation amount (%)
From 99.98% to 100%	Up to 8 minutes 38 seconds a month	Uncompensated
Less than 99.98%	Over 8 minutes 38 seconds a month	0.5% the deduction from the Customer's balance for every 30 minutes of compensated downtime, up to 100% the Balance amount.

5.1. Service unavailability (downtime) is defined as the period of time starting the moment a ticket is sent to the Executor's tech support to the moment the Executor completes work restoring the service.

5.2. Compensation is defined as the transferring of funds from the Executor to the Customer's Bonus Balance for service unavailability as outlined in Table 1. The transfer will occur within the first 7 (seven) working days of the month following that within which the violation occurred. Funds from the Bonus Account may only be used to pay for the given Service. Compensation shall be expressed exclusively as the transferring of funds to the Customer's Bonus Account.

5.3. When calculating compensation amounts, funds previously added to the Customer's Bonus Balance by the Executor (in the framework of a promotional offer or as compensation for the violation of SLA) shall not be considered when the Executor removes funds from the Customer's Bonus Balance to cover payment for the services defined in the Contract and subject to this Agreement.

5.4. In the event the Executor provides data on the start of downtime which indicates a time earlier than that shown on the ticket, this time may be used. Disagreements regarding downtime shall be resolved by negotiations between the Parties via Ticket System. In the event the Executor has no information regarding the start of downtime and no ticket is sent, the service is considered available and compensation shall not be paid.

Calculations are made independently for each virtual machine. Downtime is calculated to an accuracy of one minute. If downtime occurs at midnight between the end of one month and the beginning of the next, then the downtime will be attributed to the month when the majority of the downtime occurred. When calculating downtime for working hours, working hour limits are applied; when calculating downtime for nonworking hours, the total amount of downtime (i.e. during working and nonworking hours) is applied.

5.5. Compensation shall not be made for service unavailability related to planned maintenance. The maximum period of time a machine shall be disconnected for to perform planned maintenance and the notification period is defined in section 3.3.5.

5.6. Compensation shall not be made for:

- downtime caused by disruptions outside the Executor's area of responsibility
- downtime caused by Customer's actions;
- third party's actions;
- downtime related to scheduled maintenance;

[1] * No downtime

- the suspension of services due to the relevant request by a state structure in accordance with the current legislation;
- lost profits;
- moral harm; or
- damages caused by natural disasters.