General Terms and Conditions for Cloud Hosting Services by QSS d.o.o. Sarajevo

Introduction

Dear users,

In this document, you can find standard terms and conditions for the Cloud services provided by QSS d.o.o. Sarajevo.

General terms and conditions for Cloud services are susceptible to changes and amendments without prior notice.

By using Cloud services provided by QSS d.o.o. Sarajevo, you are automatically accepting general terms and conditions for their use.

Basic terms:
Service Provider – company QSS d.o.o. Sarajevo
User – purchaser of Cloud services provided by QSS d.o.o. Sarajevo
Contract – mutually signed contract, confirmed order or accepted offer or order made by e-mail
Update – installation of security patches released by software manufacturer
Upgrade – installation of new/newer version of software
Software – application program/tool, used as operating system, e-mail server, Web server, program language and other components which are making up the overall functional solution.
Cloud service – all products provided on "Backend" infrastructure of Service Provider, which serves as the platform of virtualization.
SLA uptime – service availability analyzed on a monthly basis
Downtime – unavailability of service on a monthly basis
VPS – Virtual private server, allocated hardware resources within Cloud infrastructure, which are forming the virtual server of the User
IaaS – "Infrastructure as a Service" - User gets all required resources including storage, CPU, RAM, NAT, Firewall, Operating System, and then creates and adjusts infrastructure as a whole by himself, on a "Backend" infrastructure provided by Service Provider.
Shared hosting – shared platform for Web or e-mail server, intended for serving multiple Users.
Spam – unwanted or unauthorized e-mail message, send to multiple recipients, which can contain malicious software, links or malicious words.
Newsletter/Bulk marketing – every e-mail message which has more than 100 recipients.

Article 1. – Service Provider Obligations

Service Provider is obliged to provide uninterrupted Cloud services to all of its Users.

Service Provider is obliged to provide services defined by the agreement/contract, confirmed by User's order, or by acceptance of Service Provider's offer.

Service Provider reserves the right to notify the User in writing, if he notices that there are online Web applications intended for a wider use by the owner of a website which are related to the commercial business or online business, but which are not included in the standard shared Web hosting package. Service Provider retains the right to notify the User in writing, if he notices that within the specific Web or e-mail hosting package, amount of e-mails being sent (Email/Bulk marketing, bulk newsletter) is larger than the amount allowed for the classic shared hosting.

Service Provider is not taking the responsibility for the functionality of User's website, if there is an issue caused due to an error in the programming/ coding (ASP, PHP, JSP, HTML etc.), except in the case where Service Provider is an author of User's website, or in a case where hosting server's components don't support all technologies required for the normal functionality of a User's website. In a latter case, Service Provider will install components if they are supported by the hosting platform and the system.

Service Provider is obliged to provide all Cloud services from its data center, located in the premises of QSS d.o.o. Sarajevo, at the address Dejzina Bikića bb, 71000 Sarajevo, Bosnia and Herzegovina.

Article 1a.

Maintenance and Uptime

Maintenance and uptime refer to regular maintenance of the equipment as well as to urgent cases (unplanned work).

Service Provider is obliged to plan and to regularly inspect and service the equipment (hardware and software). In case of planned prolonged service downtimes, Service Provider will previously notify the User, 24 hours beforehand at the minimum. Service Provider will also make a public announcement at the QSS's official "Support" portal: https://support.qss.ba. Prolonged service downtime is defined as any downtime that is longer than 5 minutes.

In urgent cases (unplanned work and unplanned service downtime) Service Provider will attempt to resolve the issue before previously notifying the Users. In that way, priority is given to the troubleshooting.

Service Provider will not treat as the downtime/ service unavailability the following cases: Planned and announced maintenance of the network and networking components

Planned and announced maintenance of the hardware components
Planned and announced maintenance of the software components
Malicious attack on Service Provider's data center (DOS, DDOS, DNS Flood, etc.)

Service Provider guarantees for SLA uptime for the 99% service availability for all of its Cloud services.

In case of unplanned and unforeseen downtimes of Cloud services, in other words, in case of non-fulfillment of the base SLA uptime, Service Provider is obliged to refund the percentage of the monthly fee for the used service, by applying the following guidelines:
100% - 99.90% uptime: /
99.89% - 99.80% uptime: refund 5% of a monthly fee for the paid service*
99.79% - 99.70% uptime: refund 10% of a monthly fee for the paid service*
99.69% - 99.60% uptime: refund 15% of a monthly fee for the paid service*
99.59% - 99.50% uptime: refund 20% of a monthly fee for the paid service*
99.49% - 99.00% uptime: refund 30% of a monthly fee for the paid service*
98.99% - 97.00% uptime: refund 60% of a monthly fee for the paid service*
96.99% - and below uptime: refund 70% of a monthly fee for the paid service*

*Monthly fee includes a fee for the paid service explicitly, without any additional options which can be bought as the service add-on.

In order to provide the refund, Service Provide must receive a written request from the User (e-mail, fax, letter addressed on the Service Provider's address), submitted within the 7 days from the day of the service breakdown.

For the official complaint related to the availability of the specific service, in other terms – uptime of the SLA time, Service Provider explicitly uses the following:
internal monitoring system, configured with the WAN access protocol,
external monitoring system of the independent company which is provider of the particular type of monitoring services (uptimerobot.com).

All information, upon User's complaint or request, can be provided through these monitoring systems, and these are the only valid evidence which can be used to determine the adequacy of the submitted complaint.
Monitoring analyses used by the User or by the third parties (providers of the monitoring services), will not be accepted, nor analyzed by Service Provider's staff, because of the following reasons:

Service Provide can't fully determine if all servers of a third party, provider of a monitoring services, were online and had a free access through its providers and sub providers, so that the sent package could reach the QSS's data center,
Service Provide can't fully determine in which way it was monitored and what amount of details contains the report of the service used for to monitor User's website/ application (all sent and received packets by User's monitoring system provider).
Service Provider can't fully determine if there are packets which haven't reached the Service Provider's data center at all, but which are part of User's SLA calculation (used for monitoring by the monitoring service, such as icmp – ping, http, SMTP and similar services), or if requests for checkups sent from the User's server (or more precisely, from third party's server) possibly lost, and where, as well as on which hoop (sub provider) these data were lost.
Service Provider can't fully determine in which way the User's monitoring service provider generates and calculates downtime – unavailability of website/ service, as well as which is the defined time – http connect, http delay check, which are comprising the calculation of the SLA uptime.

Article 2. – User's Obligations

User is obliged to make sure that software and applications which are used as the platform of his website or the Cloud service, and especially free "Open source" software (Joomla CMS, Drupal CMS, WordPress, etc.) are regularly upgrade and updated with the actual (stable) versions, in order to prevent the potential unpermitted third party access to the hosted website through the known flaws of the previously mentioned software (bugs, critical issues, code injection, vulnerabilities and other issues). Service Provider isn't responsible in a case of an intrusion to the User's website, due to the failure of a CMS system, or due to the insufficient protection of such system by the User.

User (as well as the other entities engaged or authorized by the User) is explicitly responsible for the technical functionality of his website, Cloud service, as well as for the development of his website, adjusted script or coding (CGI, PHP, Perl, HTML, ASP, etc.), as well as the content of a website, except in the cases when it is defined differently by the agreement.

If user's web page or VPS server contains unauthorized scripts/files recognized as malicious and threats to the site itself, web server or cloud platform, the service provider will inform the user and recommend that they be removed.
The customer is obliged to act according to the service provider's instructions and immediately approach the problem.

If the customer does not resolve the problem within 3 days from the moment when problem was reported by the service provider, the service provider reserves the right to temporarily remove (suspend) the web page or VPS server until the customer resolves the problem.

The service provider reserves the right to immediately temporarily shut down the service or modify access to service data if there is a direct breach of the security of the web server or cloud platform.

The user is exclusively responsible for his/her content and files constituting His/Her site or VPS server, as well as the solutions used to create/configure a web site/portal (CMS tools - content management system).

The content, design and the purpose of User's website are solely defined by the User. The User has to respect the limitations set by the general terms and conditions and regulatory provisions. Under the same conditions, during the term of the contract, User may conduct modifications or updates to the website.

The User is obliged to notify the Service Provider if he/she plans to use the shared hosting to deliver the larger quantities of e-mails (e-mail/bulk marketing, bulk newsletter), in the amounts which are over the defined limits for the shared hosting packets (Article 7.).

Sending of spam e-mails is explicitly prohibited and it entails consequences in terms of shutting off the e-mail user or the e-mail domain from the e-mail server, without the possibility of reactivation; as well as the contract termination without the additional obligations from Service Provider towards the User. The User is fully responsible for all the damage that may be cause by the transmission of spam e-mail messages.

The User is obliged to keep the password confidential, i.e. to protect it from the abuse by the third party.

The User must not jeopardize the functionality nor impose the damage to the Service Provider's network and resources, which are available to him/her within the boundary of using the given Cloud service. Furthermore, the User must not disturb the other users of the service, nor use the Cloud service in a way that may cause disturbance to the other users.
The User is responsible for the unauthorized access to the copyright or to the industrial property rights of third parties. The User is also responsible for the unauthorized access to the other information and resources as well as for carrying out illegal actions.

The User is obliged to comply with every act of general terms and conditions as well as to every other term provided by the Service Provider, instructions and notifications which are related to the proper use of the Cloud service.

Use of any sort of software or tools which can cause adverse consequences is strictly prohibited, including use of:

- tools for bitcoin mining;
- IRC/Chat tools;
- torrent trackers;
- spamming software;
- tools for carrying out malicious attacks;
- tools for detection and abuse of Cloud platform's vulnerability and other resources which are needed for running the service;
- tools for the network scanning and scanning of Service Provider's or other users' resources;
- game servers.

Service Provider retains the right to declare a particular software as harmful, in regard to the previous classification, in case that there is a need for such procedure.

The User must be aware of the fact that Service Provider's network and resources which are available to him/her through the Cloud service remain exclusively Service Provider's property. The User holds rights to use the service, without the possibility to transfer these rights to the third parties on any legal basis. The User must not allow the third parties to use the capacities or network resources as well as other Service Provider's resources, which are provided to the User through the Cloud service.

The User must not exploit the server access, i.e. use it in any way that may cause the damage to the Service Provider, server or other users which also use the server. The user must not use the hosted resources for the hacker attacks and for the exploitation of the possible security flaws of the system. Furthermore, User must not conduct any kind of investigation for the purpose of giving confidential information about the server to the third parties, nor use the resources in any way that opposes to the general terms and conditions.

Article 3. – Hosting, User's responsibilities, Permissible Behavior and Misconduct

All services of the Cloud hosting must be used for the purposes which are permitted by the law. It is strictly prohibited to transfer, store or present information, data or materials which are prohibited by the law in the Service Provider's country, as well as in the User's country. This includes, but is not limited to: materials which violate the copyrights or trademarks, materials which violate the business secret, protected patents, public regulations etc.

The content of the Cloud hosting and web presentation is considered as prohibited, especially in the following cases:

- if it's used in the conduct of crime or economic violation;
- if it violates copyrights or trademarks;
- if it leads to the unfair competition;
- if it violates third party's rights;

- if it violates business customs or consumer protection rules;
- if it violates terms of the contract, convention and recommendations in the field of telecommunications laws, as well as the code of conduct on the Internet.

According to the accepted code of conduct, some of the behaviors which are prohibited are:

- distribution of unsolicited or unwanted e-mails;
- use of service for the unauthorized access or use of service for getting access to the other systems on the Internet;
- spamming Service Provider's server by sending identical unsolicited e-mails to the large number of addresses on the Internet;
- preventing the uninterrupted use of the service by other users; preventing the uninterrupted use of Service Provider's network or any other network or part of the Internet;
- sending and forwarding charitable requests, petitions, chained e-mails, advertising and promotional materials for products and services, except to the places which are predicted to be used for these type of advertising;
- distribution of viruses or other (malicious) programs with infecting and destructible properties.

It is strictly prohibited to publish the content which points to the use of narcotics, criminal, publishing of protected passwords, illegal activities or other information which can lead to disruption of the security of Service Provider's server, as well as to the charges related to the previously mentioned content. It is also prohibited to publish, send or transfer any sort of offensive, racist, chauvinistic content.

Any attempt to disrupt the Service Provider's network or any of its components is strictly prohibited. Disruption of system's or network's security may lead to the civil lawsuit or criminal responsibility. Service Provider will investigate events which can lead to such violations, in a cooperation with a law enforcement authorities.

These disruptions include, but are not limited to:

- Unauthorized intrusion to other user's account;
- Attempt to disrupt any other service with through "flooding", DOS/DDOS attacks, "mail bombing" and similar;
- Making changes to any part of TCP/IP package;
- Any activities which lead to obtaining the access to the service for which originally User doesn't have usage rights.

Prohibited uses of shared hosting also include:

- Use of dynamic program scripts on servers, whose execution lasts more than 60 seconds;

- Use of unusually large number of bases or tables on a server the database is located at;
- Use of SQL requests in a program scripts for whose execution is needed disproportionately large part of memory (RAM) or processor (CPU) resources;
- Use of the hosting server for proxying traffic from one server to anther;
- Sharing of contents which include peer-to-peer protocol.

Furthermore, following actions aren't allowed on a shared hosting servers as well:

- direct access by RDP/SSH protocols
- direct and remote access to the database server, databases;
- direct access to the operating system, components of the servers and applications which make the web hosting service;
- direct access to the logs which are system logs, operating system level logs, or applications which make the web hosting service.

Previously mentioned items related to the database administration and review of the logs are provided by the Service Provider through the hosting panel.

Shared web hosting servers will not be customized and customized to the individual request of the user. They are configured, tuned and optimized by the Service Provider. If the User has special configuration requirements, he can order dedicated VPS servers.

The User is exclusively responsible for the overall content, appearance and purpose of the leased service, and is solely responsible for the eventual prohibited content or the purpose of it.

If Service Provider finds out that the User or unauthorized third parties are abusing the leased service, or if the Service Provider receives a complaint from the third parties about the misuse of the leased service, in accordance with the terms of general terms and conditions and legal norms, the leased service will be automatically suspended. The User will be notified in writing, until the final resolution of the problem has been made.

All eventual costs incurred to the Service Provider's due to the abuse of the service shall be completely paid by the User.

The User shall hold a copy of the published content on his/her computer. In case of unforeseen disaster, caused by the force majeure or User's mistake, Service Provider isn't responsible for the eventual data loss. Service Provider isn't responsible for material or immaterial damage, caused due to tardiness, interruptions or mistakes on communication links on the Internet, and communication links towards ISP providers, in announced or unannounced form.

If there are announced works of the third party, Service Provider is obliged to notify the User that there is a chance for interruption of the Internet service. Service Provider takes the responsibility for ensuring that the access to the servers is reliable and safe as possible, with the minimum number of interruptions.

By accepting the general terms and conditions, User takes the responsibility for excluding the Service Provider in any case where claim for the damage may be made due to the User's violation of general terms and conditions. The User is obliged to compensate any amount which Service Provider pays to the third parties as compensation for the occurred damage.

Article 4. - Copyrights and Ownership Rights, Protection of the Information and Privacy, Business Secret

Service Provider is obliged to respect the privacy of the User. The files which make the content of the web hosting and Cloud service shall be left to the User's discretion. If the need arises for the additional interventions, which are not included in the leased service, whereas there is a reasonable suspicion that there is a threat to the system's, User's and Service Provider's security; Service Provider retains the right to inspect the User's files of substantial character, which are in a direct relation with the system and its functionality, for the purpose of removing the security issue.

Service Provider will protect all entrusted information and documents which are User's property, and if the request arises, destroy them after the completion of service.

Contracting parties, including all of their employees/ associates and authorized persons are obliged to keep all of the documents and the data which are related to the subject of the contractual lease as the business secret, as well as all the data about the other party which are not generally known and to which they've gained access through the conduction of agreed service.

Contracting parties are obliged, in accordance with positive regulations, to protect the privacy of the User, except in the case of violation of general terms and conditions. Service Provider is obliged to use all the User's data that is received through the use of the Cloud service, only for the purpose of the legal business. Furthermore, Service Provider will not process or forward the personal data to the third party without the permission of the User, except in the case of the official duty, or to the parties which are authorized by the special regulations.
If User of Cloud services has the specific requests which are related to the copyrights or the ownership data, protection of the personal data, legal acts of Bosnia and Herzegovina, he/she can require from the Service Provider – QSS d.o.o. Sarajevo, mutual authorization of such, specific requests.

Business secret must be kept in privacy, by the both contractual parties upon termination of the contractual relationship.

Article 5. – Service Provider's Limitations of Liability

Service Provider is not liable for the eventual congestion, delay or errors in the functioning of parts of the Internet, on which Service Provider can't objectively make an impact. Service Provider is not responsible in any way for the content, appearance and purpose of User's website or the Cloud service, and especially for business results and consequences resulting from use of these two; as well as for the accuracy of the information and other materials which User receives from the third parties/ website visitors.

Service Provider is not responsible for the validity and execution of the contracts which, through his/her website or the Cloud service, User concludes with the third parties.

Service Provider is not responsible for User's website or Cloud service security, in terms of their invulnerability by the third parties on the Internet, and for website access rights for the third parties on the Internet. Service Provider is also not responsible for the eventual damage done to the website, Cloud service or to the User by the third parties on the Internet.

Article 6. – User's Exclusive Responsibility

The User is responsible criminally, civilly and in any other way for the prohibited content, appearance and purpose of his/her website, e-mail content or the Cloud service. The User corresponds to the Service Provider for every damage occurred due to the prohibited content on his/her website or the Cloud service.

Article 7. – "Fair-use" of Hosting Services

"Fair-use" definitions:

This section corresponds to the packages of Cloud hosting where web hosting package and general limitations which apply to all web hosting packages, are not defined by the contract.
A.) Web domain

1. Web domain space (website presentation) doesn't exceed 10GB of server's hard disk space;
2. Base (sum of all bases) of web domain doesn't exceed 1GB;
3. Bandwidth (transfer traffic of website's visitors) of web domain doesn't exceed 65GB;
4. Web domain (website and presentation) doesn't more than 10% of overall webserver's memory and processor resources (RAM and CPU).

Furthermore, this section also corresponds to the Cloud e-mail hosting packages where e-mail hosting package and general terms and limitations which apply to all e-mail hosting domains of shared hosting packages, are not defined by the contract.

b.) E-mail domain

1. E-mail domain space (one e-mail domain – all e-mail accounts) doesn't exceed 10GB of server's hard disk space;
2. Number of e-mail addresses (e-mail accounts) of one domain doesn't exceed 300 e-mail addresses;
3. Maximum size of an e-mail message is limited to 25MB (megabytes);
4. Maximum number of mailing lists for one e-mail domain is limited to 5, whilst size of an e-mail message which is sent to the mailing list must not exceed 200KB (kilobytes);
5. Exclusive responsibility of an e-mail account's end user is planning, archiving and keeping of his/her e-mail messages and contacts which operate on Service Provider's web or mail server. After creating an e-mail account, the User will be provided will all necessary instructions and recommendations. These can be also found on the technical support portal: https://suppports.qss.ba;
6. Service Provider is not responsible for archiving, storing and keeping the User's e-mail messages, except in the cases where it is otherwise defined by the contract;
7. If User of the website, application or the e-mail server (e-mail account or mailing list) performs sending of notices/newsletter to more than 300 e-mail addresses, he/she is obliged to notify the Service Provider, so that they can mutually find a solution for use of this type of service. Classic shared hosting is not intended for e-mail marketing services, bulk marketing, newsletter and similar;
8. The User of classic shared hosting package can send up to 100 e-mails within one hour – 60 minutes;
9. If User owns a personal e-mail server on his/her own infrastructure (Microsoft Exchange, Lotus Domino and similar), SMTP filtering and relaying of e-mails via Service Provider's infrastructure (SMTP filters, e-mail servers), except in the cases where it is otherwise defined by the contract. For such service, Service Provider offers a commercial service, and User can additionally order and use this type of service;
10. In cases where User of an e-mail hosting owns a web hosting (website) on a personal in-house or web server (that is not on Service Provider's infrastructure), which is used for sending e-mails, notifications, newsletter or e-mail marketing from that web server/portal, SMTP filtering or e-mail relaying from Service Provider's infrastructure is not included. The User is obliged to deliver these e-mails from his/her website or own server which is not on the Service Provider's infrastructure;
11. By default, every web hosting package includes an option of basic antivirus and antispam filtering, with the 85% - 95% detection rate for the known viruses, Trojans and spam messages. Optionally, the User can order a separate service – Enterprise SMTP filtering (Cloud Email Security), where the detection rate is between 99% and 99,9% for

the known viruses and spam messages, as well as additional options for protection such as IP reputation filtering etc. User should have an antivirus/antispam software installed on his PC. He/she is also obliged to familiarize with the general terms and conditions for the use of an e-mail service, as well as with the method of work of an e-mail service. The User should not open e-mail messages or attachments with the unknown names or extension from e-mails that are sent by unknown senders.

12. Authentication credentials (username and password) must match with the information of an e-mail sender.

In cases where the previously stated "Fair-use" options are exceeded, as well as the items from other articles written in this document, Service Provider will contact the User, present the statistics of his/her web or mail domain, and suggest appropriate solution for his/her web or mail domain needs.

Article 7a. – General Information and Limitations of an E-mail Extensions

As preventive and security protection of e-mail users, Service Provider has blocked certain extensions within an e-mail or e-mail attachment, which circulate through the e-mail traffic (incoming and outgoing). Extension that are potentially carrying high levels of threat and which are blocked on level of an e-mail server and SMTP filters are:

exe-ms, exe, vbs, pif, scr, bat, cmd, com, cpl, dll, lha, cab, rpm, cpio, tar, jar, sis, mrc, 386, ad, ade, adp, app, asp, bas, chm, crt, docm, fxp, grp, hlp, hta, inf, ini, ins, isp, jar, js, jse, lib, lnk,mda, mdb, mde, mdt, mdw, mdz, msc, msi, msp, mst, ocx, ops, pcd, prg, reg, sct, shb, shs, sys, vb, vbe, vss, vst, vsw, vxd, ws, wsc, wsf, wsh.

Since Service Provider uses the third-party software (antivirus and antispam manufacturers) for antivirus, antispam, reputation and e-mail filtering for standard and enterprise hosting, which work on principle of automatic definitions, rules and patterns released by third party software manufacturers, Service Provider can't guarantee that the e-mail message which circulates in these antivirus/antispam systems will not be declared as spam/potential spam or virus/potential virus. Service Provider is not responsible if an e-mail message which circulates in SMTP filter system is marked or declared incorrectly (false positive or false negative).

There is so-called "local quarantine" or "outbreak quarantine" on certain SMTP filter systems, where certain e-mail messages, declared as potential messages with threat are stored. Such messages can be quarantined up to 24 hours, depending on the used third party software. In this period, these messages are scanned multiple times with the antivirus and antispam software, including the new definitions/patterns received from the antivirus/antispam software manufacturer. After spending 24 hours in quarantine, depending on the outcome of the automatic antivirus and antispam scan, e-mail message will be declared as spam or virus,

deleted or delivered to the final destination. Subject of such e-mail messages can include notices such as “Suspected Spam!”, “Suspected Spam or Virus!” or similar, which should indicate to the final user to be careful with these e-mail messages. The User should pay attention to the sender, and should not open the messages from unknown senders, nor the attachments – if he/she is not sure that they are from the trusted sources (senders). The User is responsible for the outcome of opening such messages or attachments of such messages which can contain malicious software (Trojan, virus, key logger etc.).

Service Provider can’t technically of functionally have an impact on all settings of antivirus and antispam software which he uses, and especially not on the RBL (RealTime Blackhole List) providers or their declaration of IP addresses, IP subnets or e-mail messages as spam or similar; as well as on the software which is used as SMTP filter, which is manufactured as it is, by its manufacturer.

Article 7b. – Limitations of PHP Directives

As preventive and security protection of web servers and websites, Service Provider has blocked specific PHP directives which are representing potentially huge threats to the web server and websites.

PHP directives which are blocked on the PHP configurations are:
dl,exec,furl_open,passthru,pfsockopen,popen,posix_kill,posix_mkfifo,posix_setuid,proc_close,proc_open,proc_terminate,shell_exec,system,leak,posix_setpgid,posix_setsid,proc_get_status,proc_nice,show_source,phpinfo,escapeshellcmd,ini_restore,base64_decode,decode_base64,base64_url_decode,str_rot13,rot13,apache_child_terminate,curl_exec,curl_multi_exec,apache_setenv,define_syslog_variables,posix_getpwuid,pcntl_exec,syslog,chgrp,chown,chmod,pclose,escapeshellarg.

Article 8. – Backup of Cloud Infrastructure, Web and E-mail Server and Backup as a Service (BaaS)

Service Provider is regularly carrying out the backup of the Cloud infrastructure, web and e-mail servers. These backup copies, as well as restore of these copies, aren’t included in the User’s Cloud service.

The User can do the backup through the hosting panel, and if needed, store the backup to the web server or local computer, without any additional charges.
The User can request from the Service Provider backup or restore of his/her website or e-mail messages. Service Provider will analyze if there are technical preconditions for the request and then notify the User about it. This service is charged additionally.

Service Provider also offers additional service in form of Backup as a Service (BaaS).

Enterprise backup, intended for Users of IaaS and VPS services, represents additional service which is available for an order – Backup as a Service (BaaS). This service is presented to the User through the corresponding self-service portal which contains possibility of monitoring of backup processes and the freestanding virtual machine, individual files, databases and similar, depending on the leased BaaS package.

For this service, Service Provider uses the third-party enterprise backup solution.

Service Provider is liable to keep the backup system in the operating state and on a latest version, as well as to notify the User in case that unplanned error happens during the backup procedure.

Service Provider is not responsible for the flaws or errors within the backup software provided by the third party.

Service provider is not responsible for the correctness of the restored backup in case when the User does the backup of the virtual machine, operating system or the resources which already corrupted – already have the error.

Article 9. – Virtual Private Server Options, Semi and Fully Managed

Self Managed VPS server

Virtual private server ordered by the User will be supplied as self-managed virtual private server by the Service Provider. The User is obliged and responsible for the maintenance, administration, update and troubleshooting of potential problems caused by the faulty operation of the software, application, content etc., on his/her self-managed virtual private server.

Semi-Managed Virtual Private Server

Users who order the virtual private server with the semi-managed option from the Service Provider, will enjoy the following benefits:

- Basic monitoring and maintenance of the virtual private server (hardware, operating system and the basic configuration of the existing server);
- Basic monitoring and maintenance of all operating system's components during the process of delivering the virtual private server to the User with installed and configured modules at the time of the handover.

Semi-managed option doesn't include the following:

- Installation of service packs for the operating system, upgrade of the operating system or the software;
- Installation and upgrade of the components, applications and program technologies (IIS, Apache, .Net, .ASP, .PHP, .JSP, SQL, MySQL, PostgreSQL and other components which are not listed here);
- Installation of third-party applications and software;
- Maintenance of third-party applications and software;
- Diagnostics and debugging of a third-party application and software;
- Troubleshooting of all previously mentioned items.

Fully-Managed Virtual Private Server

Users who order the virtual private server with the fully-managed option from the Service Provider will have the benefits in terms of the maintenance, update of the operating system and its components, with the slogan: “Concentrate on your business, leave your web server to us!”.

Fully-managed option includes the following:

- Standard monitoring and maintenance of the virtual private servers and services (fully managed support);
- Monitoring of server’s load;
- Basic website functioning issues (Internal Server Errors, 404s etc.);
- Server’s networking problems;
- Issues that may emerge during server’s restart
- Hardware related issues;
- Installation of packets that are supported by the operating system (yum, rpm, windows update);
- Software upgrade and migration of versions of installed components (PHP, ASP, MySQL);
- Troubleshooting of problems emerged on an existing server configuration;
- Basic firewall setup and troubleshooting.

Fully-managed option doesn’t include maintenance of the following:

- Installation and configuration of User’s websites;
- Installation and configuration of so-called third-party CMS and scripts (WordPress, Joomla etc.);

Fully-managed option also doesn’t include the following:

- Troubleshooting or issues on User’s application (website, online application);
- Installation, maintenance of User’s applications (website, online application);
- Troubleshooting and debugging of issues related to the website’s or online application’s functionality;

- Troubleshooting of compatibility of the third-party applications or software with the web server;
- And everything else that is not mentioned above.

General Information for All Virtual Private Servers

Service Provider will notify the User if he notices large and prolonged use of server's hardware components (CPU, RAM), on a level of backend virtualization cloud platform, and accordingly give him/her suggestions on how to find an eventual problems and solutions for them.

Login credentials for the virtual private server (username and password) will be exclusively provided to the purchaser, in other words, User of the virtual private server. The User of virtual private server is responsible to protect of his/her login credentials from a third party's misuse. If User distributes his/her login credentials to the third parties, he/she accepts all outcomes and consequences of such actions, which can directly impose an impact to the server, applications and the work of an overall system.

User of virtual private server can request from the Service Provider to intervene on a server or in the operating system for the sake of debugging the potential issues in server's operation. Potential interventions will be coordinated with the User, whereas Service Provider will attempt to resolve the reported issues (request for intervention) in a documented way, if there are technical possibilities for that. Requests for intervention are charged as per actual pricelist for the Service Provider's technical support. Primary unit of billing period of intervention is 30 minutes.

RBL – RealTime Blackhole List

The User of virtual private server and the vCloud service with the self-managed option is responsible for the regular status checkups of the IP addresses that are allocated to his/her virtual private server or vCloud core. Through the IP address checkup, User should determine whether one of IP addresses allocated to him/her, are listed on the one of RBL lists. For the checkup, User can use commercial or free services such as:
http://mxtoolbox.com/blacklists.aspx;
http://www.anti-abuse.org/multi-rbl-check/.

In case that IP address is listed on one of RBL lists, the User is obliged to make a request for removal, based on the instructions of that RBL provider. In case that the User's IP address is on one of the RBL lists, Service Provider will notify the User about the status of his/her virtual private server or vCloud core, more precisely, about the status of IP address(es) allocated to his/her service.

If User doesn't make a delisting request within a 72-hour timeframe, once when he/she received notification from a Service Provider or RBL provider, Service Provider will terminate the provided service – in other words, service will be blocked until the IP address gets whitelisted, i.e. gets the "clean" or "OK" status.
In case that User's virtual private server of vCloud core become so-called zombie, spam or phishing server, Service Provider will notify the User and immediately (and eventually permanently) terminate that service.

Tabular overview of virtual private server (VPS) options and additional explanations:

OPTIONS	SELF MANAGED	SEMI MANAGED	FULLY MANAGED
Initial server setup	YES	YES	YES
Initial server update	YES	YES	YES
VPN / RDP / SSH Access	YES *vpn	YES *note1 *vpn	YES *note1 *vpn
Maintenance of initial setup of operating system and its components	NO	YES	YES
Initial setup of domain and DNS zone	NO	YES	YES
Periodical update of an operating system	NO	YES	YES
Periodical upgrade of an operating system	NO	NO	YES
Periodical update of hosting software (option with the hosting panel)	NO	NO	YES
Basic monitoring and maintenance which includes all operating system's components during the delivery of virtual private server to the User, with installed and configured modules at the time of a handover.	YES	YES	YES
Update and upgrade of components, applications and program technologies supported by the operating system (IIS, Apache, .NET, .ASP, .PHP, .JSP, SQL, MySQL, PostgreSQL and other components which aren't mentioned)	NO	NO	YES
*VPN – Option VPN is possible with every purchased Enterprise Firewall option or Cloud service IaaS			
*note1 – by default, in semi and fully-managed virtual private server options, VPS/RDP/SSH access option is not available for the User. In agreement with the User, such access to the virtual private server may be enabled.			

Your QSS Cloud hosting team!

E-mail: support@qss.ba
Support portal: https://support.qss.ba/

Remark: all the details related to the individual service as well as for the terms of use are listed on a contract signed by the Service Provider and the User.

UPDATE
03.06.2021.: Article 2. Added paragraph 3, 4, 5
07.01.2020.: business address change
28.11.2019.: Addition to the Article 3. added paragraph customization of share / shared servers
20.07.2016.: Addition to the Article 7a. blocked extensions of e-mail attachments
04.05.2016.: Correction of typos, addition of terms, changes to terminology and addition of clearer definitions in the overall documents;
01.02.2016.: Update of SLA uptime tables, correction of typos;
13.01.2016.: Update of Article 7a.
04.01.2016.: Addition to the Article 8. – RBL (Realtime Blackhole List)
30.12.2015.: Added Article 7b., update of a tabular overview of virtual private servers (VPS)
27.11.2015.: Addition – SLA maintenance and uptime (definition “monthly fee”)
15.10.2015.: Addition to the Article 7. “Fair-use”, item 11., added item 12..
07.10.2015.: Addition to the monitoring description – monitoring supervision
28.08.2015.: Update of SLA uptime description
13.08.2015.: Added a new Article – Introduction
06.08.2015: Update of extensions from Article 7a.
19.05.2015.: Added Article 7a.
30.01.2015.: Amendments and updates of the “Fair-use” definition, amendments and updates of self-managed virtual private server, additions to the tabular overview of virtual private servers, correction of typos
14.10.2014.: Amendments and updates of SLA uptime, amendments and updates of virtual private server (VPS) description, amendments and updates of the “Fair-use” definition