SERVICE TERMS AND CONDITIONS

The Service Terms and Conditions are common for all Clients.

The Service Terms and Conditions define the Agreement entry procedure and the main terms to be adhered to by the Parties in the course of discharging the Agreement for provision of the Client-selected services by the Provider. In case of any discrepancies between the Agreement wording and the text of the present Service Terms and Conditions, the latter shall prevail.

The qualitative and quantitative criteria for Provider's obligations in delivery of the Services to all Clients are specified in the Service Level Agreement contained herein.

The Provider's Services may be used for lawful purposes only.

The Provider may immediately suspend or delete any website, account, database or another server component, it if fails to comply with the present Terms and Conditions.

The Provider may immediately discontinue provision of the Services for the Client and terminate the Agreement, if the Client violates one or more clauses hereof. In this case, the funds remaining on the Client's account shall not be returned. Rendering of the Services shall be resumed upon Client's written request containing information about the measures taken to eliminate the violations and guarantee avoidance of such violations in future.

If the Client fails to meet the Services payment obligations, the Provider shall resume rendering of the Services after the Client makes payment.

Upon fee accrual, the Client shall pay for the whole traffic payable according to the Service Orders and transmitted in the course of Services rendering, including maintenance traffic necessary to ensure routing and bundling of data.

1. Service terms and conditions for virtual web hosting and web hosting on dedicated servers

1.1. The following is prohibited for the Client while using the Services:

- Using the Services for purposes contrary to law; transfer, distribution or storage of any illegal materials and information, as well as any other actions contrary to applicable laws or governing regulations, including, without limitation, infringement of copyright, illegal use of trademarks and brands, disclosure of confidential state and commercial information without authorization of the information owner, violation of export and import laws, incitement to racial or national intolerance, pornography distribution etc., via the Services.

- Unauthorized (i.e. without express authorization of the owner) access or using of resources (i.e. services, networks, systems, data, and information); breach, alteration, bypassing or damage to resource access control systems (i.e. authentication, authorization, billing, and system monitoring); attempts to scan, test, and search of means to breach or bypass resource access control systems without special authorization of the owner; interception, monitoring, alteration or forwarding of data and traffic unauthorized by the owner; interference in normal operation of services, networks, channels, and systems, including mail bombing, flooding, system overload attempts, and broadcast attacks also targeting Client's resources; alteration, modification of the address part and contents of network data packages, including email messages; any other types of access or resource usage performed for purposes or in a manner not authorized expressly by the resource owner, using the Services.

- Unauthorized distribution of commercial and other information, unreasonably persistent distribution of advertising, information or commercial materials in breach of the established rules for commercial information without the receiver's consent, as well as distribution giving rise to receiver's complaints.

- Distribution of information harmful to the reputation of and demeaning to third parties, using the Services.

- Intended damage, using the Services.

- Forging of service information in the headers of the messages sent via email, as well as entering of false personal or address information upon Client registration by the Provider; using identification data (names, addresses, telephone numbers etc.) of third parties, except where the Client is authorized by the third parties to use such data.

- Using interfaces and protocols not specified in the regulatory documents effective in the territory of the Republic of Cyprus in the Provider's network, as well as use of addressing systems failing to comply with recognized international standards specified by IANA and ICAN.

- Deployment of systems or system elements for maintenance, calculation, and use of digital currencies (cryptocurrency mining, distributed platforms, generation of new blocks providing the ability to obtain remuneration in the form of new units and fees etc.).

- Publication or distribution of any information or software containing computer viruses or other equivalent components.

  - *Information noise (spam) restrictions:*

    o Bulk messaging via email and other means of private information exchange (including such instant messaging services as SMS, IRC etc.), except when such messages are sent at the apparent and explicit initiative of the receivers. Open-access publication of an email address or another private information exchange system may not constitute a basis for including an address to any bulk messaging list. Inclusion of an address obtained by any means (through a web form, subscription bot etc.) to a messaging list is allowed only subject to the availability of a proper subscription confirmation

procedure ensuring inclusion of an address to any list only at the discretion of the address owner. The subscription confirmation procedure shall prevent an address from inclusion to any messaging list (single or regular) at the initiative of third parties being other than the address owners. It is necessary to enable any Client to leave a messaging list immediately without any difficulties, if the Client wishes to do so. Besides, the existing ability to leave a list may not legitimize inclusion of addresses to such list against the will of their owners.

    o Sending of email and other messages containing attached files and/or having significant size without the preliminary consent of the addressee.

    o Distribution of the following (unless explicitly authorized by the receiver):

        ➢ email and other messages (including single messages) of advertising, commercial or agitational nature;

        ➢ letters and messages containing rude and offensive terminology and sentences;

        ➢ messages requesting forwarding to other available users (chain letters).

        ➢ Using impersonal ('role') addresses otherwise than for the intended purpose specified by the address owner and/or standards.

- Publication of off-topic messages at any electronic conference. Hereinafter, the "conference" shall mean Usenet teleconferences (news groups) and other conferences, forums, and messaging lists.

- Publication of advertising, commercial or agitational messages at any conference, except where such messages are explicitly allowed by the conference rules or publication of such messages was pre-approved by the conference owners or administrators.

- Publication of articles containing attached files at any conference, except where such attachments are explicitly allowed by the conference rules or such publication was pre-approved by the conference owners or administrators.

- Using own or provided information resources (mailboxes, email address, WWW pages etc.) as contact details to perform any of the actions described above regardless of the Internet network point where such actions were performed.

  - *Technical support of spamming, namely:*

    o intended scanning of information resources' contents for purposes of harvesting email addresses and addresses of other messaging services;

    o distribution of spamming software;

    o development, verification, maintenance or distribution of address databases of email and other messaging services (except when the owners of all the addresses in such database explicitly approved inclusion of their addresses into this particular database; open-access publication of an email address may not be considered such approval).

- Attempts of unauthorized access to Internet resources, network attacks, and network hacking, including participation in such activities, are prohibited, except when attacking a network resource is explicitly authorized by the resource owner or administrator. The following is also prohibited:

  ○ Actions aimed at compromising normal operation of the Network components (computers, other hardware or software) not owned by the user.

  ○ Actions aimed at unauthorized accessing a Network resource (a computer, other equipment or information resource), subsequent use of such access, as well as destruction or modification of software or data not owned by the user without approval of the owners of the software or data or administrators of the information resource. Unauthorized access shall mean any access granted with the means other than those assumed by the resource owner.

  ○ Transfer of meaningless or useless information to Network computers or equipment, creating unwanted traffic for such computers or equipment, and to intermediate Network section to the extent exceeding the minimum value required to check network connectivity and availability of its components.

- It is prohibited to use dedicated servers for deployment of systems or system elements for maintenance, calculation, and use of digital currencies (cryptocurrency mining, distributed platforms, generation of new blocks providing the ability to obtain remuneration in the form of new units and fees etc.).

    1.2. In order to check adherence to the specified safety purposes and requirements and license restrictions, the Provider reserves the right to occasionally scan the files deployed by the Client on the Provider's hardware. The Provider may authorize in the Client's systems and use any software for automatic accounting to exercise the described right. Therefore, the Client shall not block this access (deactivate the account, change the password and access rights, delete/change the ssh key) and/or otherwise hinder Provider's activity (block Provider's access to the resources on the local machine and in the network, delete/complete process, deactivate startup).

    1.3. The Provider reserves the right to suspend activity of any account, if such activity causes unreasonable overload of the computing resources.

    1.4. When rendering web hosting services on dedicated servers, the Provider may, in addition to the other rights state above, remove the equipment installed and adjusted to provide the Client with the Services, if the Client fails to effect proper payment within 3 (three) calendar days after suspension of Services rendering. In case the equipment provided by the Client and installed at the Provider's site is removed by the Provider due to violation of the obligations by the Client, the Provider accrues

fixed monthly payments during the Services suspension period and the Client shall effect such payments. In order to resume rendering of the Services under the Agreement, the Client shall pay the arrears, penalty, and cost of equipment reinstallation/readjustment. The Provider shall not be liable for integrity of Client's data since equipment removal. Removed equipment may be handed over to other Clients of the Provider; in this case, resuming of Services provision on this equipment is impossible.

1.5. When rendering virtual hosting services, the Provider may suspend this service, if the Client fails to timely pay for the Services under the Agreement. Moreover, in case the Client fails to pay outstanding arrears, within 14 days since suspension of Services rendering, the Provider removes the Client's Service. Within the period from suspension of the Services under the Agreement due to failure to pay/partial payment of their cost and until the Client's Service is removed or Service rendering is resumed, the Client shall pay the amount equal to the Services cost for a similar period.

The period of Services suspension for the specified reasons shall not be considered a break in Service rendering and may not be construed as default on Provider's obligations under the Agreement.

2. Terms and conditions for allocation of IP addresses

2.1. If the Agreement includes allocation of IP addresses for the Client, the Client shall fill in a special RIPE form at Provider's request. If the Client does not use all or some of the allocated IP addresses for over a year since commencement of Services rendering, the Provider may raise the question on the necessity of the allocated number of IP addresses for the Client; should the Client have no such necessity, the Provider may delete registration of all IP addresses (a pool of IP addresses) and allocate fewer IP addresses according to the actual Client's needs. In this case, the Provider shall notify the Client about the allocated number of IP addresses via email. Should the Client require more IP addresses during the term of the Agreement, the Client may request the Provider to allocate more IP addresses.

3. Terms and conditions for issuing SLL certificates

3.1. An Order for issuing an SSL certificate shall be placed, using the Account (a private section of the Provider's website). The following shall be specified in an Order: the certificate type, validity period, CSR query, as well as any other information necessary to issue a certificate. The Client guarantees reliability of all the data specified.

3.2. The Client guarantees functioning of the mail box specified in an Order as the "Email for Confirmation" during the entire period of Services rendering.

3.3. The Client shall confirm to be entitled to control the domain name an SSL certificate is issued for.

3.4. The Provider may request additional information and documents and/or require confirmation of previously provided scanned documents and/or links to business references, as well as require translation of all the information into English during the entire period of Services rendering. Should the Client fail to provide additional information and/or confirm previously provided information at Provider's request, the Provider may decline an order or withdraw an SSL certificate. If an order is declined or an SSL certificate is withdrawn, the advance payment shall not be refunded.

3.5. The Provider shall proceed to issuing an SSL certificate after receiving payment in full and provided all the necessary documents, information, CSR query are submitted to the full extent. Issuing a certificate may take up to 30 days, depending on the certificate type. The Provider may engage third parties for Services rendering.

3.6. The Provider shall be deemed as discharged its obligations under the corresponding Order upon sending an issued SSL certificate to the Customer to the "Email for Confirmation"

3.7. The Client shall bear all the risks and be fully liable for using an issued SSL certificate.

3.8. The Provider shall not be liable for any losses (including loss of profit) incurred by the Client as a result of Service rendering and withdrawal of an SSL certificate during its validity period.

3.9. In case it is impossible for the Provider to discharge its obligations due to the Client's fault, the Services shall be paid in full.

4. Registration, prolongation, and transfer of domain names by the Provider

4.1. A consumer-oriented characteristic for operation of domain names (DNS) may be integrated into the computing environment in order to enable addressing to the computing environment via Internet and identification of network nodes.

4.2. The Provider may engage third parties for registration, prolongation, and/or transfer of domains.

4.3. The terms of registration, prolongation, transfer, and other actions related to domain names are stated in the Agreement, herein, and the rules established by domain name registrars in the corresponding domain name zone (hereinafter referred to as the "Registrar"). The Client is notified that registration data is public information in certain domain zones and anonymization of registration data may be charged in addition.

4.4. In case of registration, prolongation or transfer of a domain name, the Client shall read and understand the rules of registration and use of domain names in corresponding zones and specify true information in the application before filing the registration application.

4.5. The Client acknowledges and accepts that the Registrar may directly contact the Client or its specified representative regarding verification of the contact data, domain name prolongation according to the procedures established by authorized organizations.

4.6. The Client shall be fully liable for prolongation of the domain names registered to the Client.

4.7. The Provider may independently choose a registrar for maintaining the information about the corresponding domain name and delegate such responsibilities among registrars during registration, prolongation, and transfer of a domain name.

1. GENERAL INFORMATION

2.   This document specifies additional qualitative and quantitative criteria for Provider's obligations in delivery of the Services to all Clients.

2. AREAS OF RESPONSIBILITY OF THE PROVIDER AND CLIENT

2.1. The Provider's warranties shall apply only to the Provider's area of responsibility including the following:

- Provider's communications center;
- exterior communication channels leased and/or owned by the Provider up to the interfaces with the communication centers belonging to other communication service providers directly connected (by a single cable) with the Provider's equipment, as well as up to the interfaces with the local networks integrating various communication service providers directly connected (by a single cable) with the Provider's equipment;
- Client's lines, if they are provided to the Client by the Provider;
- termination equipment (physical server components), if such equipment is installed for the Client by the Provider as part of the Services and controlled by the Provider.

2.2. Instances of DDoS attacks are excluded from the Provider's area of responsibility. In case of a DDoS attack on the Client's server, if such attack significantly affects normal operation of the network equipment, the Provider may block access to the Client's server from Internet during the attack.

2.3. All other system elements are within the Client's area of responsibility, including installation and setting of server and application software, information security, data backup and recovery systems.

2.4. The Client shall be solely liable for the contents of the information processed by means of the Services, transferred by the Client or a third party under the Client's network credentials via Internet and Provider's own resources, for information integrity, freedom from third-party claims, legitimacy of information distribution, and the damage caused by the Client's actions (personally or by another person under the Client's network credentials) to the personality or property of citizens, legal entities, states.

2.5. The Provider does not guarantee absolute reliability or accuracy of the Services and does not warrant that the software offered or any other materials are free from computer viruses and other malicious components. The Provider undertakes all reasonable actions and measures to prevent this.

2.6. The Provider shall not be held liable for quality of the public communication channels used to access the Services.

2.7. The Client assumes full responsibility and all the risks related to using the Internet Network via the Provider's resources and/or services.

2.8. The Provider shall not be held liable for notifying any third parties about restriction of Client's access and for the potential consequences caused by the absence of such notification.

2.9. In case of termination of Services rendering, the Provider shall not be held liable for notifying or failure to notify any third parties about restriction of Client's access and for the potential consequences caused by such notification or absence thereof.

2.10. The Client shall be fully liable for security of its Login and Password and for the losses resulted from unauthorized use of the Client's Login and Password; in particular, the Provider shall not be held liable for disclosure and/or compromising of the Client's credentials by the Client. Any person that sends the Provider the information used for Client identification (for example, answers to security questions, SMS codes, calls from/to verified phone numbers etc.) and other information used for authorization in the Billing System may be considered by the Provider as a Client's representative acting on its behalf. All actions performed by such person shall be deemed to be direct actions of the Client.

2.11. If the Client independently uses hardware and software for protection of its information resources, the Client shall be fully liable for reliability of such protection and losses caused by unauthorized access of third parties.

2.12. In order to check adherence to the specified safety requirements and license restrictions, the Provider reserves the right to occasionally scan the files deployed by the Client on the Provider's hardware. The Provider may authorize in the Client's systems and use any software for automatic accounting to exercise the described right. Therefore, the Client shall not block this access (deactivate the account, change the password and access rights, delete/change the ssh key) and/or otherwise hinder Provider's activity (block Provider's access to the resources on the local machine and in the network, delete/complete process, deactivate startup).

3. SUPPORTING PROCEDURE

3.1. Technical support

3.1.1. The Provider renders technical assistance on the matters related to provision of the Services specified in the Service Orders by communication/correspondence with the Client in electronic format, using the Support Center section of the Provider's Billing System.

3.1.2. Technical support includes the following operations and consultations:

- management of the Client's Services (server reboot, operating system reinstallation);
- ISPmanager control panel (consultations on the panel operation, elimination of configuration errors);
- settlement of issues with popular services (WWW, MySQL, Mail, DNS, FTP).

3.1.3. System administration operations not described in cl. 3.1.2. can be performed only after preliminary approval by technical support specialists in electronic format, using the Support Center section of the Provider's Billing System. Certain operations can be performed on a paid basis. The terms and conditions of the Agreement shall not apply to the speed and quality of such performing operations.

3.1.4. All the technical consultations specified are not included in the consultations related to programming, web designing, and teaching of skills of working in Internet and using the Services.

3.2. Information support

3.2.1. Information support implies receiving of reference information about the services provided, rates, client request processing rules, and domain names.

3.2.2. Information support is provided via instant messaging tools on the Provider's official website (Live Chat), email, applications created in the Provider's Billing System.

3.2.3. If the Client files a request 1 (one) hour before the end of working time or later, the Provider may respond to such request on the next business day.

4. SPECIFICATION OF TARGET SERVICE-QUALITY LEVELS

4.1. Service activation time

4.1.1. After the Provider receives payment for the Service under the Agreement and initiation of Service processing, access to the Service is granted within 1 hour for the Virtual Hosting and Dedicated Virtual Server Services and within 24 hours for the Dedicated Server Services.

4.2. Guarantee service uptime

4.2.1. The Provider guarantees the minimum Service availability of 99.9 % at the end of a month (maximum 43 minutes of unavailable access to the Service according to the information from the Provider's monitoring system). The unavailability Service period is calculated from the moment the Client registers such request at the Provider's system. The Service availability parameter excludes the time spent for scheduled operations related to hardware and software upgrade of the server or other equipment in the process area, as well as for unscheduled operations announced via email.

4.4. Emergency situations, response time

4.4.1. In case of hardware and software failure of the server or other equipment in the process area, the maximum failure correction time shall be 24 hours since the moment of problem detection.

4.4.2. Detection of a failure fact takes place at the moment the Provider receives a Client's request for failure rectification or at the moment registered directly by the Provider.

4.4.3. The equipment installed for the Client by the Provider in the course of Services rendering shall be replaced by the Provider at no extra charge, unless the Client fails to adhere to the provisions of the Agreement, as well as in case of other wrongful actions of the Client. The Provider may temporarily install another type of equipment to replace faulty equipment, unless it deteriorates the quality of the Services provided for the Client.

4.5. Maintenance operations

4.5.1. Scheduled maintenance operations are always performed, when Internet user are least active. Service access may be restricted temporarily during maintenance operations.

4.5.2. In case of performing scheduled preventive maintenance by the Provider or other organizations, assuming the Provider was aware of such maintenance, the Provider shall notify the Client about such operations via email or the Provider's official website not later than 24 hours before commencement of the operations (except for unexpected and unscheduled operations aimed at repair and preventive maintenance).

5. REIMBURSEMENT AND SETTLEMENT OF DISPUTES

5.1. If one of the Agreement clauses stated above is not adhered to due to the Provider's fault, which prevents using of the Services by the Client, the Provider shall recalculate the fixed monthly fee at Client's request. Recalculation shall be made from the moment and upon receiving of a Client's application by the Provider with allowance for the duration of the Services rendering interruption and to the extent of 1/30 of the fixed monthly payment for the interrupted Services, if the interruption time exceeds 43 minutes per month. Interruptions in Services rendering exceeding 43 minutes shall be rounded to 1 day. Interruptions in Services rendering lasting less than 43 minutes shall not be considered for recalculation. The amount of compensation is limited to 100% of charges for the Service for the calendar month in which the quality of the Service was breached.

5.2. Reimbursement is effected in the form of extending the period of services provision with consideration of the calendar month results. Reimbursement under this clause of the Agreement shall be effected, only if the Provider's Services are timely paid by the Client.

5.3. To receive reimbursement, the Client shall file an application, using the Support Center section in the Provider's Billing System, within one calendar month from the moment of the Provider's default that prevented using of the Services by the Client for a period exceeding 43 minutes.

5.4. No reimbursement is made in the following cases:

- if services are provided in the test mode;
- if service interruption is caused by Client's violation of the provisions stated in the Agreement and attachments thereto;
- occurrence of force majeure;
- performance of scheduled and unscheduled maintenance operations announced to the Client within the prescribed time;
- for periods of suspension of the Service, as well as the facts of termination of the Service, removal of the Service or termination of the Agreement caused by the violation by the Client of the provisions of the Agreement;
- complete or partial inability to take any actions with the Service through the control panel, account, via api, as well as using other management tools, while maintaining the availability of the Service;
- for periods of unavailability of the Services associated with failures outside the Provider's area of responsibility, including (but not limited to): network attacks (DDoS, SYN, "mail bomb", etc.), errors in the operation of the domain name system, inoperability of Internet network segments;
- other circumstances outside the Provider's area of responsibility.

6. FORCE MAJEURE CIRCUMSTANCES

6.1. The Parties shall be indemnified from the liability for partial or complete failure to discharge their obligations under the Agreement, if such failure results from occurrence of force-majeure events after entering into the Agreement. In particular, the Parties consider the following circumstances to be force majeure: accidents causing integrity damage to the Provider's network; interruption in power supply of the Provider's active equipment; acts of God; natural and industrial disasters; acts of terrorism; military operations; civil disorders; adoption by state or local authorities of resolutions containing prohibitions or restrictions on the activities of the Parties under this Agreement; other circumstances that cannot be foreseen or avoided and prevent the Parties from discharging their obligations under the Agreement.

The Parties shall immediately inform each other about occurrence of any circumstances that hinder or otherwise affect performance of the Agreement upon receiving of such information.

6.2. In case of occurrence of force majeure circumstances hindering fulfillment of the obligations under the Agreement, the time of fulfillment of the obligations by the Parties shall be postponed for a period corresponding to duration of such circumstances, including the time required to eliminate the consequences, up to a maximum of 60 (sixty) calendar days. If force majeure circumstances remain in effect for a longer period or both Parties clearly understand the force majeure circumstances will remain in effect for a longer period, Parties shall discuss potential alternative ways to perform the Agreement or terminate it without reimbursement of damages. In this case, the Provider shall return the funds not used under the Agreement to the Client.