CLOUD COMPUTING AGREEMENT

Terms of Service

These terms of service (the "Terms of Service") apply to and are a legally binding agreement between Cyber Internet Services (Pvt.) Ltd., a Pakistani limited liability company ("Cybernet") and the Customer (as defined below).

The Terms of Service, the Service Level Agreement ("SLA") and the Order (defined below), form an agreement ("Agreement") between Cybernet and the Customer and relates to Cybernet's business being run in the name and style of 'RapidCompute' which essentially provides cloud computing services ("RapidCompute"). This Agreement governs all services provided by RapidCompute to the Customer and is effective from the moment (i) the Customer indicates agreement on the RapidCompute Website by clicking "I agree" or "Submit", or (ii) the two parties sign a written Agreement in person (whichever comes first).

1. Definitions

In these Terms of Service, unless there is something inconsistent to the subject or context, the following words and expressions shall have the meaning respectively assigned to them as follows:

1.1 "**Affiliate**" shall mean and include an entity that now or in the future, directly or indirectly controls, is controlled by or is under common control with a party to the Agreement.

1.2 "**Agreement**" shall mean and include the "Cloud Computing Agreement" between both the parties as defined in the recitals above.

1.3 "**Control**" shall mean the ownership of more than fifty percent (50%) of the

(i) voting power to elect the directors of the said entity, or
(ii) ownership interest in said entity.

1.4 "**Infrastructure As A Service (IAAS)**" is a Cloud Computing service model that refers to delivery of computer infrastructure on an outsourced basis to support enterprise operations. IAAS typically includes provisioning of basic computing infrastructure resources (e.g. physical and virtual machines, datacentre space, network bandwidth, storage, network components, software in the form of operating system etc.).

1.5 "**Customer**" means the entity or individual named on the Order including End Users, and Website visitors.

1.6 "**CDE**" means Cardholder Data Environment

1.7 "**Customer**" means the entity or individual so named on the Order including End Users, and Website visitors.

1.8 "**Customer Data**" means any data (including but not limited to any software application) stored by the Customer on the infrastructure provided by RapidCompute in connection with the Services.

1.9 "**Cloud computing**" means the availability of infrastructure (CPU and Memory, Storage and Network Transfer), platforms and applications. The key features of cloud computing include the possibility of quick provisioning, deployment and scaling up or down of the cloud components. This allows the customers to use IT resources over the Internet instead of physically owning them, thereby creating solutions that are robust, cost effective and accessible through one computer with Internet connectivity.

1.10 "**Customer Technology**" means Customer's proprietary technology, including without limitation, all text, pictures, sound, video, and log files, Customer's software (in source and object forms), user interface designs, architecture and documentation (both printed and electronic), know-how, and any related Intellectual Property Rights throughout the world (whether owned by Customer or licensed to Customer from a third party).

1.11 "**End Users**" means any person or entity deriving use of the Services through the Customer including but not limited to the Customer, an Affiliate of the Customer or a customer of the Customer.

1.12 "**Force Majeure Event**" is any event beyond either party's reasonable control, including, without limitation, acts of war, acts of God, earthquake, hurricanes, flood, fire or other similar casualty, embargo, riot, terrorism, sabotage, strikes, governmental act, insurrections, epidemics, quarantines, inability to procure materials or transportation facilities, failure of power, restrictive governmental laws or regulations, court orders, condemnation, failure of the Internet or other event of a similar nature.

1.13 "**Governmental Authority**" means any federal, national, state, regional, county, city, municipal, local, territorial, or tribal government, whether foreign or domestic, or any department, agency, bureau or other administrative or regulatory body obtaining authority from any of the foregoing, including without limitation, courts, public utilities and communication authorities.

1.14 "**Intellectual Property Rights**" means and includes any and all intellectual property of whatever nature and kind including without limitation patents, registered designs, trademarks and service marks (whether registered or not), rights in the nature of unfair competition rights, copyrights, database rights, design rights, and all similar property rights including those subsisting (in any jurisdiction) in inventions, designs, drawings, performances, computer programs, semi-conductor topographies, confidential information, business names, goodwill and the style and presentation of goods or services and applications and the right to apply for protection of any of the above rights.

1.15 "**Mark-up Rate**" means a penalty rate of 5% per month.

1.16 "**Monthly Recurring Charges**" or "**MRC**" means the fixed charges payable to Cybernet by the Customer on a monthly recurring basis for the use of the Services.

1.17 "**Network**" means the telecommunications network, including but not limited to fiber and optical and wired/wireless transmission equipment, which is owned and/or leased and operated and maintained by Cybernet or its Affiliates.

1.18 "**Order**" means the order submitted by Customer to RapidCompute via the Website or any other means acceptable to Cybernet setting out matters relating to RapidCompute's delivery of Services to the Customer and governed by these Terms of Service.

1.19 **"PCIDSS"** means Payment Card Industry Data Security Standard.

1.20 "**Personal Information**" means any information that may identify a particular individual.

1.21 "**Service(s)**" means those services provided by Cybernet –RapidCompute division to the Customer which allow the Customer to store data and/or use the Software via the infrastructure provided by RapidCompute as further described in the Order.

1.22 "**Service Fees**" means charges for the Services (including but not limited to Monthly Recurring Charges and non-recurring charges) as identified in the relevant Order.

1.23 "**Service Level Agreement**" or "**SLA**" means the service level provisions describing the service level targets as mentioned in the SLA document.

1.24 "**Software**" means any software application provided by RapidCompute which the Customer may have license to use in accordance with any Order.

1.25 "**Technology**" means Cybernet's proprietary technology, including but not limited to, RapidCompute Services, software tools, hardware designs, algorithms, software (in source and object forms), user interface designs, architecture, class libraries, objects and documentation (both printed and electronic), network designs, know-how, business methods, and graphic images and text made available on the Website, trademarks, logos, domain names and any related Intellectual Property Rights vested in Cybernet pursuant to the Copyright Ordinance, 1962, and any other applicable laws.

1.26 "**Website**" means the RapidCompute website available at **www.rapidcompute.com**

2. Service Conditions

2.1 General

The Customer may submit an Order(s) which shall constitute an offer to buy the Services. Cybernet may then accept the offer at its sole discretion at which time both parties will be legally bound to the Agreement. Acceptance may occur by:

i) a message received via the Website acknowledging receipt and acceptance of the Order; or
ii) delivery of the Services

Except as otherwise agreed by the parties, Cybernet shall not be obligated to accept any Order.

2.2 Term and Termination

2.2.1 Termination or Suspension by either Party

a. The term of this Agreement shall be for an indefinite time period and shall remain effective unless the Agreement otherwise terminates in accordance with the provisions hereof.

b. Either party may terminate and discontinue Service serving **three (03) months** written notice period to the other party. The same shall apply to termination of individual services as mentioned in Annexure B.

c. The termination of this Agreement by either Party for any reason whatsoever would not waive Cybernet's right to recover the outstanding amount/charges from the Customer subject to the terms and conditions of this Agreement.

d. In cases where the Customer's Services are suspended due to non-payment, Cybernet maintains the right to terminate the Customer's Services by providing written notice in the form of a pending invoice to the Customer seven (07) days prior to termination of the Services.

e. In cases where the Customer violates the Terms of Service or any other policies mentioned on the Website and other RapidCompute, Cybernet maintains the right to terminate the Customer's services by providing written notice to the Customer two (02) days prior to termination.

f. In cases where the Customer's account remains inactive for more than thirty (30) days, Cybernet reserves the right to terminate the account by providing a written notice seven (07) days prior to termination.

2.2.2 Additional Termination or Suspension by Cybernet

Cybernet solely shall have the right, upon written notice, to immediately terminate and /or suspend any Order(s), and/or discontinue or suspend the delivery of the affected Services (without liability) in the event that:

(a) Customer has violated any law, rule, regulation or policy of any government authorities related to the or Customer's or an End User's use thereof, or **Sections 3** or **4.6** (acceptable use policy and anti-bribery); or

(b) In the event RapidCompute division receives any direction, notification, or instruction from any Governmental Authority (or any independent Internet content monitoring entity) to suspend or terminate the provision of Services to Customer (through no fault or negligence of RapidCompute Division).

2.2.3 Cybernet's Remedies

In the event Cybernet terminates an Order because of any reasons set forth in **Section 2.2.2**, then Customer agrees to pay to Cybernet the fixed Monthly Recurring Charges and / or any other fixed minimum charges for the remaining of the initial monthly term or the current monthly renewal term.

2.3 Fees

Cybernet shall charge the Customer Services Fees as detailed in **Annexure A**. Cybernet shall be entitled to increase or decrease its Service Fees upon a thirty (30) day prior written notice to Customer.

2.4 Billing and Payment

Unless otherwise agreed between the parties in writing, billing for Services shall be done in either monthly or on such other payment period as is listed in the Customer's Order, for a package of services listed in the Order.

Cybernet shall invoice all Service Fees as per the Order of the Customer not later than the 10th day of such period and Customer shall pay the due amount within fifteen (15) days of date of such invoice. With reference to **Annexure B**, Customer may increase ("**Upgrade**") its Services package through the RapidCompute Customer portal, "**my1.RapidCompute.com**" (the "**Customer Portal**"). Additional charges will go into effect upon Upgrade, and Cybernet may charge a pro-rated increase in Service Fees for the payment period during which the Upgrade occurs, on a daily basis (or at such times as it chooses).

Services will renew automatically at the end of its period. If the period is one month or less, Customer may cancel the services two (02) days prior to the next billing cycle through the Customer Portal.

If the period exceeds one month, Customer may cancel the services at any time during the first 30 days of a renewed period, and if Cybernet has already charged Customer for such period, it will refund the fees, pro-rated to deduct the time between the start of the period and cancellation.

The Customer will provide notice of cancellation through the Customer Portal.

Any amount due but not received by Cybernet will accrue Mark-Up Rate from sixteenth (16) day after the date of invoice to the date of payment, at the Mark-up Rate (pro-rated on a daily basis). Furthermore, Cybernet shall have the right to set off any amounts due hereunder which are not paid when due against any amounts owed to Customer or its Affiliates by Cybernet or its Affiliates pursuant to these Terms of Service or any other agreement between the Parties.

2.5 Taxes and Fees

Customer will be responsible for payment of all applicable VAT, GST, consumption tax, use, excise, access, bypass, franchise, regulatory or other similar taxes, fees, charges or surcharges, whether now or hereafter enacted, however designated, imposed on or based on the provision, sale or use of the Services (hereinafter "**Taxes**").

To the extent Customer is or believes it is exempt from payment of certain Taxes, it shall provide to Cybernet a copy of a valid exemption certificate. Cybernet will give effect to all valid exemption certificates in the next full billing cycle following receipt of the certificate from Customer, but only to the extent Cybernet is permitted to do so under applicable laws. Notwithstanding the foregoing, in the event that a Customer exemption certificate is or becomes invalid during the term of any Order, and Cybernet is assessed or responsible for additional Taxes, penalties or late charges, Customer shall be responsible for such charges in accordance with this **Section 2.6**.

If a Customer deducts withholding tax from payment made to Cybernet, the Customer commits to providing evidence of such deduction to Cybernet for further claims as advance taxes. If any taxing or Governmental Authority asserts that Cybernet should have collected certain Taxes from Customer which Cybernet did not collect, Customer hereby agrees to indemnify Cybernet for such Taxes and hold Cybernet harmless on an after-tax basis from and against any Taxes, interest or penalties levied or asserted in connection therewith.

2.6 Disputed Bills

In the event Customer disputes in good faith any portion of RapidCompute's invoice, Customer must pay the undisputed portion of the bill and submit a written claim for the disputed amount, documenting the basis of its claim. All claims must be submitted to Cybernet within fifteen (15) days of receipt of billing for such Services. Customer acknowledges and agrees that it is able to and that it is reasonable to require Customer to dispute bills within that time and Customer therefore waives the right to dispute the charges not disputed within the time frame set forth above.

2.7 Software Licenses

Customer may be provided with the right to use certain Software which shall be governed by the terms of the relevant Software license terms available at the Website. Customer agrees, acknowledges, and authorises Cybernet to enter into the relevant Software license in Customer's name as a client to satisfy any Software license terms and third-party Software license terms so as to accomplish any Services of Cybernet pursuant to this Terms of Service. Customer agrees and acknowledges that Cybernet is not renting any client software to Customer.

2.8 PCIDSS Compliance

For customers that are hosting a PCIDSS v3.2.1 compliant CDE on RapidCompute's infrastructure, RapidCompute will maintain all applicable PCIDSS requirements to the extent that it possesses or otherwise stores, processes, or transmits cardholder data on behalf of the customer, or to the extent that it could impact the security of the customer's cardholder data environment. These requirements will be applicable as part of the shared hosting environment and RapidCompute shall also maintain the additional Service Provider controls for this environment. Details of the shared hosting environment, the scope applicable to the CDE and responsibility shall be mutually agreed and documented as an addendum to this agreement. For all PCIDSS CDE, the applicable standard shall be PCIDSS 3.2 or the current applicable PCIDSS standard as mandated by the PCI Council.

2.9 Demarcation of Responsibilities

For the avoidance of doubt, Cybernet is only responsible for providing the management of the server host hardware including storage and a web-based portal for overall management of the Service and, if requested by Customer and agreed by Cybernet, the provision of the Software.

The Customer is responsible for managing and operating the Software including but not limited to patch management, upgrades, antivirus, system security, application programs and data. The Customer is also responsible for managing and configuring its use of the Service (via the Website and other portals provided) including but not limited to, user access administration, security controls and payment information.

3. Acceptable Use Policy ("AUP")

3.1 General

Cybernet does not control or monitor the content of the Customers' online communications, however, Cybernet may edit or remove content, with prior intimation of three (03) days, that it deems to be in violation of the AUP or that it otherwise deems to be harmful or offensive.

Each Customer is responsible for preventing violations of this AUP by third parties accessing the Service through Customers' computers or accounts, including without limitation, hackers and Customers' own users. No credit will be available under this Agreement for interruptions of service resulting from AUP violations.

If Customers engage in conduct while using the Services that is in violation of the AUP or is illegal or otherwise improper in Cybernet's sole discretion, Cybernet reserves the right to suspend and possibly terminate Services provided by RapidCompute or the Customer's access to the Services. In most cases, Cybernet will attempt to notify Customer of any activity in violation of the AUP and request that the Customer cease such activity; however, in cases where the viability of the Services are potentially threatened or cases involving unsolicited commercial emails / SPAM, mail relaying, alteration of Customer's source IP address information, denial of service attacks, illegal activities, harassment or copyright infringement, Cybernet reserves the right to suspend / restrict the Customer's access to the Services at Cybernet's sole discretion, without notification.

In addition, Cybernet may take any other appropriate action, legal or otherwise, against a Customer for violations of the AUP, which may include termination of the Service. Customer will reimburse Cybernet for any expenses resulting from Customer's violation of the AUP, including attorneys' fees. Customer is responsible for the use of its Services, including use by hackers and other unauthorised third parties. Customer's responsibility includes payment for exceeding transfer and bandwidth limits.

Except where RapidCompute division specifically accepts such responsibility in the Order, Customer is responsible for maintaining security, including disaster recovery systems and backups. (Customer is advised to maintain its own backups outside of Cybernet's premises and systems, even if RapidCompute provides backups, security, or other services related to data protection.)

The Services must be used in a manner that is consistent with the intended purpose of the Services and may be used only for lawful purposes. Customers shall not use the Services in order to transmit, distribute or store material:

(a) in violation of applicable Laws of Islamic Republic of Pakistan regulation, including export or encryption laws and other regulations;
(b) that may adversely affect the Services or other RapidCompute division customers; or
(c) that may expose Cybernet to criminal or civil liability.

Customers are prohibited from facilitating the violation of any part of this AUP, including, but not limited to transmitting, distributing, or otherwise making available any product or service that violates this AUP.

3.2 Misuse of the Services

Customer shall be responsible for the Services usage and shall not use the Services nor allow the Services to be used for any unlawful or illegal purposes or to transmit, distribute or store contents or messages (including e-mail messages) which are inappropriate (including, but not limited to, obscene (including pornography), defamatory, libellous, threatening, abusive, hateful, or excessively violent), harmful (including, but not limited to, viruses, worms, password-cracking programs or Trojan horses), and/or fraudulent or misleading (including, but not limited to, false, deceptive, or misleading statements, claims, or representations), as reasonably determined by Cybernet in accordance with generally accepted standards of the Internet community, nor to transmit or distribute unsolicited e-mail messages where such e-mail messages could reasonably be expected to provoke complaints (spam).

Further, Customers are prohibited from using the service of another provider to send spam to promote a site hosted on or connected to Cybernet's Services/ Website. In addition, Customers shall not use the Services in order to:

- send e-mail messages which are excessive and / or intended to harass or annoy others,
- continue to send e-mail messages to a recipient that has indicated that he / she does not wish to receive them,
- send e-mail with forged TCP / IP packet header information,
- send malicious e-mail, including, without limitation, "mail bombing",
- send or receive e-mail messages in a manner that violates the use policies of any other Internet service provider, or
- use an e-mail box exclusively as a storage space for data.

3.3 Unauthorised or Fraudulent Use of the Service

Customer shall be responsible for (save as to the extent caused by any acts or omissions of Cybernet), taking all reasonable measures to avoid and immediately notify RapidCompute division of any unauthorised or fraudulent use of the Service. Customer shall be solely responsible for all charges incurred in respect of the Services even if such charges were incurred through, or as a result of, such fraudulent or unauthorised use.

3.4 Cooperation with Investigation Authorities

Cybernet will cooperate with appropriate law enforcement agencies and other parties involved in investigating claims of illegal or inappropriate activity covered under any law in force at that time. Cybernet reserves the right to disclose Customer information to the extent authorised by federal surveillance statutes.

3.5 Privacy

Because the Internet is an inherently open and insecure means of communication, any data or information a Customer transmits over the Internet may be susceptible to interception and alteration. Cybernet makes no guarantees regarding, and assumes no liability for, the security and integrity of any data or information a Customer transmits over the Internet, including any data or information transmitted via any server designated as "secure."

3.6 Reporting AUP Violations

Cybernet requests that anyone with information about a violation of this AUP, or of RapidCompute's Terms of Service, report it by sending an email to abuse@rapidcompute.com.

3.7 Rules of Engagement to Perform Penetration Testing on RapidCompute Cloud

Customer is prohibited to carry out the below mentioned activity without the presence of an authorized Cybernet personnel. An instance where an authorized Cybernet personnel cannot be physically present with the Customer shall be mutually discussed between both the parties.

This program shall enable the Customer to test the services hosted by Cybernet without causing harm to any other Cybernet Customer. Below mentioned services shall be prohibited on Cybernet's network.

- Scanning or testing assets belonging to any other Cybernet Customers;
- Gaining access to any data that is not wholly belong to the Customer;
- Performing any kind of denial of service testing;
- Performing network intensive fuzzing against any asset except Customer's Virtual Machine provided by Cybernet;
- Performing automated testing of services that generate significant amounts of traffic;
- Deliberately accessing any other customer's data.
- Moving beyond "proof of concept" repro steps for infrastructure execution issues (i.e. proving that you have sysadmin access with SQLi is acceptable, running xp_cmdshell is not).
- Using Cybernet's services in a way that violates the Acceptable Use Policy, as set forth in this Agreement.
- Attempting phishing or other social engineering attacks against our employees.

Customer shall be permitted to:

- Create a small number of test accounts and/or trial tenants for demonstrating and proving cross-account or cross-tenant data access. However, it shall be prohibited to use one of these accounts to access the data of another customer or account.
- Fuzz, port scan, or run vulnerability assessment tools against their own RapidCompute Virtual Machines.
- Load testing application by generating traffic which is expected to be seen during the normal course of business including testing surge capacity.
- Testing security monitoring and detections (e.g. generating anomalous security logs, dropping EICAR, etc.).
- Attempt to break out of a shared service container such as RapidCompute Websites or RapidCompute Functions. However, Customer must immediately report it to RapidCompute and cease digging deeper. Deliberately accessing another customer's data is a violation of the terms.

Apart from the prohibitions mentioned under this section, Cybernet reserves the right to respond to any on its networks that appear to be malicious. Many automated mitigation mechanisms are employed across the RapidCompute Cloud which will not be disabled to facilitate a penetration test at any point in time.

4. Obligations of the Parties

4.1 Customer's Representations and Warranties

Customer represents and warrants that:

(i) it has the legal right and authority, and will maintain the legal right and authority for the duration of the Agreement, to use the Services as contemplated hereunder;

(ii) the performance of Customer's obligations under these Terms of Service and use of the Services will not violate any applicable law, rule or regulation or any applicable manufacturers' specifications or otherwise unreasonably interfere with Cybernet's Customers' use of the Services or Network, and

(iii) the Customer is authorised and has completed all required corporate actions necessary to execute the applicable Order(s).

4.2 Cybernet's Representations and Warranties

Cybernet represents and warrants that:

(i) it has the legal right and authority, and will maintain the legal right and authority for the duration of the Agreement, to provide the Services ordered by Customer hereunder;

(ii) the performance of Cybernet's obligations under these Terms of Service will not violate any applicable law, rule or regulation; and

(iii) Cybernet is authorised and has completed all required corporate actions necessary to execute the applicable Order form(s).

4.3 Contact Information

Customer shall keep updated its contact and payment details via the RapidCompute Website and other portals at all times.

4.4 Privacy Policy

Cybernet is committed to respecting and protecting the privacy of Customers.
The Customer will provide RapidCompute division with contact and payment information. Contact information includes name, email address, postal address, and telephone number. Payment information includes a credit card number or other payment details. Customers' information will only be used to support the customer relationship with Cybernet, and will never be passed to any third party unless this is necessary to provide services to the Customer or where Cybernet is legally required to do so.
The Customer also stores and transmits data using the Services. Unless the Customer gives explicit permission, RapidCompute will never inspect Customer's stored data and will only measure the volume of transmitted data for billing purposes or inspect the transmitted data to investigate suspected violations of the Acceptable Use Policy. RapidCompute shall not disclose Customer Data to any third party unless required to do so by law.

The Customer acknowledges and agrees that Cybernet may use, process and / or transfer Personal Information of the Customer and / or its employees (including intra-group transfers, transfers to third parties and transfers between countries):

(i) in connection with the provision of Services;

(ii) to incorporate such Personal Information into databases controlled by Cybernet for the purpose of account administration, billing and reconciliation, operational maintenance and support activities, fraud detection and prevention, and customer and market analysis and reporting; and

(iii) to communicate to the Customer by voice, letter, fax or email regarding products and services of Cybernet. If Customer believes that, in the course of providing Services under these Terms of Service, Cybernet will have access to data Customer does not want Cybernet personnel to comprehend, Customer should encrypt such data so that it will be unintelligible.

Customers may send requests to amend, correct or delete personal information submitted through Cybernet's website or other portals at any time by sending an email to legalaffairs@cyber.net.pk. The support staff will take reasonable steps to verify the Customer's identity before making any such modifications.

4.5 Customer Network Security

Customer is responsible for maintaining the security of its internal network from unauthorised access through the Internet. Cybernet shall not be liable for unauthorised access to Customer's network or other breaches of Customer's network security.

4.6 Anti-Bribery

Without limiting the generality of the foregoing, under no circumstances shall Customer make, cause, or authorise any third party to make or cause any bribes, kickbacks, or illegal payments for the purpose of influencing a person's acts or decisions or in order to obtain or retain business in connection with the Services received hereunder. Customer agrees to comply with all applicable anti-bribery laws.

4.7 Export Control

The parties acknowledge that products, software, and technical information (including, but not limited to service, technical assistance, and training) provided under these Terms of Service or used by the Customer in connection to the Services may be subject to export laws and regulations of Pakistan and other countries, and any use or transfer of the products, software, and technical information must be in compliance with all applicable regulations. The parties will not use, distribute, transfer, or transmit the products, software, or technical information (even if incorporated into other products) except in compliance with all applicable export regulations. If requested by either party, the other party also agrees to sign written assurances and other export-related documents as may be required to comply with all applicable export regulations.

4.8 Data Storage and Retention

a. Customer shall delete all the data within **Ten (10)** working days upon the termination of the Agreement, once the notice period is served and the receipt of termination is acknowledged.
b. Cybernet shall delete all Customer data within **Ten (10)** working days once the timeline mentioned in Clause (a) has lapsed.
c. Customer acknowledges and agrees that Cybernet shall not be responsible for any data stored by the Customer using the Services. Notwithstanding the above, the Customer may copy such data using the Services to a separate location at any time.
d. Cybernet is only offering Infrastructure as a "service" to all its customers, and has zero visibility and/or access to customer virtual machines, storage, and other resources hosted on RapidCompute's infrastructure.
e. The personally identifiable information of all the customers will be removed and/or deleted entirely from RapidCompute's records after a "request" is generated by the Customer and there are no pending dues against their accounts. If the business transaction has not been completed, or if the pending dues are not paid/cleared before generating the request then the request would not be processed and be put at a halt.

   Nonetheless, for all financial transactions, financial accounts, and financial details of the customer, the finance department may proceed with the retention time as directed by the relevant regulatory authority.

4.9 Return of Customer Hardware Equipment

a. Customer shall collect its hardware equipment (as mentioned in Annexure B) from Cybernet Premises within **Ten (10)** working days upon the termination of the Agreement, once the notice period is served and the receipt of termination is acknowledged.

b. While coming for the receipt of the equipment, the Customer's representative shall be required to prove his identity along with the Authority letter to Cybernet. Customer must acknowledge in writing the receipt of the equipment to Cybernet.

c. Customer acknowledges and agrees that Cybernet shall not be responsible for any destruction or loss to the Customer's equipment once the timeline mentioned in Clause (a) has lapsed.

5. Ownership

5.1 Intellectual Property

Customer is and shall remain exclusively entitled to all right and interest in and to all Customer Technology and its confidential information, and Cybernet is and shall remain exclusively entitled to all right and interest in and to all RapidCompute Technology and its confidential information. Neither party shall, directly or indirectly, reverse engineer, de-compile, disassemble or otherwise attempt to derive source code or other trade secrets from the property of the other party. Customers may print copies of the information on the Website for personal use only.

Customers may not distribute any graphic images or text included herein; re-display this information on their websites or modify or re-use in any way the graphic images or text on Cybernet's website or other portals without the express written permission of Cybernet,

RapidCompute trademarks, logos and domain names are registered trademarks of Cybernet and are protected by trademark and other laws in Pakistan and other countries. Use of Cybernet or RapidCompute trademarks is prohibited unless expressly authorised by Cybernet. Customers are not permitted to use any trademarks displayed on the website, Meta tags or any other "hidden text" utilising trademarks of RapidCompute and its licensors, without prior written permission of Cybernet or such third party who may own the trademark. Without the express prior written consent of Cybernet, no Cybernet or RapidCompute trademarks may be used in a manner that implies an affiliation with, approval by, endorsement of or sponsorship by RapidCompute.

Customers wishing to use the "Powered by RapidCompute" logo may contact their respective sales account managers for further details.

Customers may not use the RapidCompute Website / other portals, material on the Website / other portals for any purpose or in any manner that infringes the rights of any third parties. Cybernet would like its customers to report any content on the RapidCompute Website / other portals that is believed to infringe any copyrights through an email to the support address.

5.2 Intellectual Property / Copyright Infringement Claims

It is Cybernet's policy to respond to notices of alleged trademark / copyright infringement according to the procedures mentioned in the relevant applicable laws.

If the complaint is about material put up by a Cybernet Customer, please note that RapidCompute is not responsible for Customer content. RapidCompute does not;

- Put up content;
- Manage such content;
- Have physical access to such content

Such matters should be taken up directly with the offending party. If an agreement cannot be reached between the complainant and the offending party, it is suggested that legal proceedings may be done against such offending party.

5.3 IP Addresses

The parties acknowledge and agree that RapidCompute may provide Customer the right to use certain IP addresses owned and/or licensed by Cybernet in connection with the provision of the Services. Customer acknowledges and agrees that on termination of the Agreement for any cause Customer's right to use such IP addresses shall automatically terminate.

5.4 Customer Data

Customer shall exclusively own all rights, title and interest in and to the Customer Data and shall bear sole responsibility for legal obligations associated with the same, including but not limited to compliance with any laws applicable to Intellectual Property Rights, regulatory compliance, accuracy, integrity and legality.

6. Liability and limitation of liability

6.1 Indemnification

Each party shall indemnify the other from any claims by third parties (including Governmental Authorities) and expenses including legal fees and court costs with respect to

(i) damage to tangible property, personal injury or death caused by such party's negligence or wilful misconduct;

(ii) a breach by either party of **Sections 4.1** and **4.2** of the Terms of Service.

6.2 Damages

Notwithstanding any other provision hereof, neither party shall be liable for any indirect, incidental, special, consequential, exemplary or punitive damages (including but not limited to damages for lost profits, lost revenues, loss of goodwill, loss of anticipated savings, loss of customers, loss of data, interference with business or cost of purchasing replacement services) arising out of the performance or failure to perform under any order or these Terms of Service, whether or not caused by the acts or omissions or negligence of its employees or agents, and regardless of whether such party has been informed of the possibility or the likelihood of such damages; provided however, that the foregoing limitations shall not apply to the parties' indemnity obligations contained herein.

6.3 Indemnity and Limitation of Liability

The Customer hereby acknowledges and agrees to monitor and/or restrict the content accessed by the Customer (or by any other party through the Customer) using the Services in order to comply with relevant and applicable laws, rules, regulations, licensing terms and conditions. The Customer hereby agrees to indemnify and keep Cybernet harmless from any loss, expenses, costs, damage or claim incurred by or occasioned to Cybernet as a result of use of the Services by the Customer or any other person or party acting or through the Customer in any manner which may be deemed to be use of the Services in contravention of any provision of applicable law, rules, regulations or licensing conditions, or in violation of any intellectual property rights and rights of privacy.

Cybernet's sole liability and Customer's sole remedy for damages arising out of the furnishing or the failure to furnish the Services (including but not limited to mistakes, omissions, interruptions, failure to transmit or establish connections, delays, errors or other defects) is limited to the payments received under this Agreement.

6.4 Disclaimer of Warranties

Except for warranties expressly made in these Terms of Service, Cybernet makes no warranties or representations express or implied, either in fact or by operation of law, statutory or otherwise, including warranties of merchantability, satisfactory quality, and fitness for a particular use or non-infringement.

7. Miscellaneous Provisions

7.1 European Economic Area (EEA)

If the Customer is a Company located within the European Economic Area (EEA) involved in controlling and processing of European Union (EU) Citizens' personalized data, it shall then comply with the terms and conditions set out in the Data Processor Agreement mentioned in "**Annexure C**" of this Agreement.

7.2 Publicity

Neither party shall have the right to use the other party's or its Affiliates' trademarks, service marks or trade names or to otherwise refer to the other party in any marketing, promotional or advertising materials or activities, provided, however, that RapidCompute shall be entitled to refer to Customer (by name and / or logo) as its customer only (no further details shall be disclosed) in any such materials or activities. Neither party shall issue any publication nor any press release relating to any contractual relationship between Cybernet and Customer except as required by law or agreed in writing between the parties.

7.3 Confidentiality

Both parties agree to take care of the confidentiality of the information gathered/obtained from the other in the due course of business and/or as a consequence of provision of the Services. This restriction shall continue to apply after the termination of services without limit in point of time. Furthermore, Confidential Information includes all information provided to a party by the other party under any Order, including without limitation technical, operational, marketing, billing, pricing and commercial information in relation to the supply of Services.

Notwithstanding the foregoing, confidential information shall not include information that:

a) is independently developed by the receiving party; or
b) is lawfully received by the receiving party free of any obligation to keep it confidential; or
c) becomes generally available to the public other than by breach of this Section.

The confidential information shall remain the property of the relevant party. Each party shall maintain the confidentiality of the confidential information of the other party using at least the same degree of care as it employs in maintaining as secret its own trade, proprietary and confidential information but in any event always at least a reasonable degree of care.

A party must not disclose the other party's confidential information to any person except:

a) to its employees (which for Cybernet -RapidCompute includes its Affiliates' and its third party service providers' employees) on a 'need-to-know' basis provided those persons first agree to observe the confidentiality of the information;
b) to legal and financial advisers;
c) with the other party's prior written consent; or

d) if required by law, any stock exchange, or any Government Authority.

7.4 Consent to Disclose

Cybernet reserves the right to provide any Customer or potential Customer bound by a non-disclosure agreement access to a list of Cybernet's Customers and a description of the Services purchased by such Customers. Customer consents to such disclosure; including the listing of Customer's name and the Services purchased by Customer (financial terms relating to the purchase shall not be disclosed).

7.5 Contents of Communications

Cybernet does not monitor and will have no liability or responsibility for the content of any communications transmitted via the Services, and Customer will indemnify, defend and hold Cybernet harmless from any and all claims (including claims by any Governmental Authority seeking to impose penal sanctions) related to such content or for claims by third parties relating to Customer's use of the Services.

7.6 Application of Tariffs

In the event Cybernet is required to file tariffs with a Governmental Authority, the terms set forth in the applicable tariff shall govern Cybernet's delivery of, and Customer's consumption or use of, such Services but only to the extent required by law, rule or regulation. In the event that there is any material change required to the Terms of Service and / or the Service Fees then Customer shall have a right to terminate the affected Services.

7.7 Force Majeure

Except for Customer's payment obligations under these Terms of Service and / or any Order, neither party shall be liable, nor shall any credit allowance or other remedy be extended, for any performance that is prevented or hindered due to a Force Majeure Event. If RapidCompute is unable to provide the Services for a period in excess of thirty (30) consecutive days for any reason set forth in this Section, then either party may cancel the affected Order upon written notice to the other party, and both parties shall be released from any further future liability under that particular Order.

7.8 Governing Law; Dispute Resolution

These Terms of Service and any Order shall be governed by the laws of the Islamic Republic of Pakistan and the parties irrevocably submit to the non-exclusive jurisdiction of the courts of Pakistan. In the event a RapidCompute invoice is not disputed and the Customer simply fails to pay, then Cybernet may seek to recover the sum due in any court of Pakistan without reference to its conflicts of law and the Customer hereby submits to the jurisdiction of any such court.

7.9 Severability; Waiver

In the event any provision of these Terms of Service is held by a court of competent jurisdiction to be invalid, void or unenforceable, such offending provision(s) shall be stricken and the remainder of these Terms of Service shall remain legal, valid and binding. The failure by either party to exercise or enforce any right conferred by these Terms of Service shall not be deemed to be a waiver of any such right nor
will it be deemed to operate so as to bar the exercise or enforcement of any such or other right on any later occasion.

7.10 Assignment

The Customer may not assign an Order without first obtaining Cybernet’s written consent. Cybernet may assign any Order(s) to, including but not limited to, an Affiliate or as part of a corporate reorganisation, consolidation, merger or sale of substantially all of its assets, or by any other means, by providing advance written notice to Customer of any such proposed assignment. Any purported assignment by the Customer in contravention of this clause shall be invalid and the Customer shall remain bound. These Terms of Service will bind and insure to the benefit of each party and each party's successors and permitted assigns.

7.11 Notice

(a) **To Cybernet:**
Any routine notice or communication must be sent using the RapidCompute Website and other portals. Any legal notice or communication can be sent by Customer by electronic email or courier, to the following address:

RapidCompute c/o Cyber Internet Services (Pvt.) Ltd.
9th Floor, Lakson Square Building No. 3
Sarwar Shaheed Road, Karachi - 74200
Pakistan
Att. Legal Department
Email: legalaffairs@cyber.net.pk
Tel: +922- 111-44-55-66

Such notice will be deemed to have been given as of the date it is sent or delivered, as applicable.

(b) **To Customer**:
Any routine notice or communication must be sent to the individual(s) nominated by Customer as its contact(s) by electronic email, courier or facsimile at the address set forth in the Order(s) or at such other address as may hereafter be furnished.

Such notice will be deemed to have been given as of the date it is sent, delivered or faxed, as applicable.

7.12 Changes to these Terms of Service

Cybernet may modify these Terms of Service upon a thirty (30) day notice to Customer upon which such modification shall be effective, provided, however, that, upon receipt of such notice Customer may terminate any Order without termination liability by delivering a written thirty (30) day notice of termination no later than thirty (30) days after the effective date of the change notification.

7.13 Third Party Beneficiaries

Cybernet and Customer agree that there shall be no third party beneficiaries to these Terms of Service or any Order, including, but not limited to, any sub-licensee or End User of Customer or the insurance providers for either party. To the extent it is allowed by law any legislation in any relevant jurisdiction giving rights to third parties is hereby excluded.

7.14 Entire Understanding

These Terms of Service, the SLA and any applicable Order(s) constitute the entire understanding of the Parties related to the subject matter hereof. All prior written or oral agreements, understandings, communications or practices between Customer and Cybernet, are hereby superseded and withdrawn and shall have no legal effect insofar as they relate to the Services hereunder. In the event of any conflict between the documents comprising the Agreement, precedence shall be given to the documents in the following order:

(i) the Order;
(ii) the SLA; and
(iii) Terms of Service.

ANNEXURE A – SERVICE LEVEL AGREEMENT

This Service Level Agreement (the "**SLA**") applies to and is a legally binding agreement between Cyber Internet Services (Pvt.) Ltd., a Pakistani limited liability company ("**Cybernet**") and the Customer. Both parties have contemporaneously entered into a legally binding Terms of Service Agreement (the "**Terms of Service**").

The SLA, the Terms of Service, and the Order, form an agreement ("**Agreement**") between Cybernet and the Customer and relates to Cybernet's business being run in the name and style of 'RapidCompute' which essentially provides cloud computing services ("**RapidCompute**"). This Agreement is effective from the moment

(i) the Customer indicates agreement on the RapidCompute Website by clicking "I agree" or "Submit", or

(ii) the two parties sign a written Agreement in person (whichever comes first).

To avoid any ambiguities, this SLA excludes Cybernet's GPON, MPLS, IP and other connectivity services as such services are covered under separate SLAs between the Customer and Cybernet. This SLA only covers the Services provided to the Customer by Cybernet.

1. Definitions

In this SLA, unless there is something inconsistent to the subject or context, the following words and expressions shall have the meaning respectively assigned to them as follows:

1.1 "**Service Downtime Credit**" means the credit provided by RapidCompute to Customer in relation to an Unavailable Service.

1.2 "**Unavailable Service**" means that Customer is unable to access its subscribed resources running on the Services platform due to failure of a critical component of the Service (including virtual server, server instance, firewall, load balancer, switch, storage platform, and connectivity to Cybernet Network services (i.e. internet and MPLS) from the Service platform); and "Unavailability" means accordingly.

1.3 "**Uptime Target**" means the target time for Cybernet's Services to be available after taking into account the impact of exclusions mentioned in **Clause 4** of this document.

Capitalised words and expressions used in this SLA, and not defined herein, shall have the meanings respectively assigned to them in the Terms of Service.

2. Service Uptime Target

The Service is provided with an Uptime Target of 99.9% for each calendar month. This means that if the Services are down for more than forty-three (43) minutes during a calendar month, the Customer will be entitled to Service Downtime Credit. Customer will only be entitled to Service Downtime Credit for such portion of the Service that is affected.

3. Service Downtime Credit

Service Downtime Credit shall be allowed to the Customer as per the following table:

Service Downtime Duration (Minutes per Calendar Month)	**Service Downtime Credit**
Up to 43 Minutes	No Credit
Additional 01 Hour	5% of Monthly Recurring Charges
Additional 02 Hours	10% of Monthly Recurring Charges
Additional 03 Hours	15% of Monthly Recurring Charges
Additional 04 Hours	20% of Monthly Recurring Charges

4. Exclusions

Following events shall be excluded from any Unavailable Service calculations;

- Scheduled/Planned maintenance activities which have been announced in advance
- Force Majeure events
- Acts or omissions of Cybernet's upstream providers or failures of the Internet
- Failures or malfunctions in Customer's software, hardware, or technology due to the negligence of the Customer.
- Unavailability due to acts or omissions of the Customer or End Users

- If the Customer is in breach of any of Cybernet's policies or the Terms of Service. This shall include, but not be limited to, the Customer's payment obligations against using the Services.
- Law enforcement activities
- Actions of third parties, including but not limited to security compromises, denial of service attacks and viruses

5. Service Downtime Credit Request Procedure

For RapidCompute to process a Customer's request for Service Downtime Credit, the Customer should send the request in writing within thirty (30) days of the event giving rise to the Service Downtime Credit. The written request must include the following:

- Description of the Unavailable Service, including date, time, and duration
- Documentation of proof of the Unavailable Service i.e. monitoring or system logs

Cybernet will be the sole arbiter regarding the award of Service Downtime Credit and Cybernet's decision will be final and binding. The award of Service Downtime Credit as described in this SLA will be the sole and exclusive remedy for Unavailability of stored data or virtual servers or loss of stored data. Service Downtime Credit will only be provided against future Services and for the avoidance of doubt may not be exchanged for cash or other forms of payment.

6. Entire Understanding

This SLA, the Terms of Service, and any applicable Order(s) constitute the entire understanding of the parties related to the subject matter hereof. All prior written or oral agreements, understandings, communications, or practices between Customer and Cybernet, are hereby superseded and withdrawn and shall have no legal effect insofar as they relate to the service levels hereunder. In the event of any conflict between the documents comprising the Agreement, precedence shall be given to the documents in the following order:

(i) the Order;
(ii) this SLA; and
(iii) Terms of Service.

ANNEXURE B – RAPIDCOMPUTE ORDER

- ***The Monthly Recurring Charges (MRC) shall be subject to the actual status of the Services or Products being used by the Customer, and such products/services' status shall be viewed in Rapid's self-service Customer Portals (https://my1.rapidcompute.com/). If the customer increases the quantity of services from the customer portal(s), then additional charges for the same will come into place, over the MRC model.***

ANNEXURE C – DATA PROCESSING AGREEMENT

1. BACKGROUND

The Data Controller (____________) and the Data Processor (_____________) are parties to this Cloud Computing Agreement where certain Personal Data concerning Data Subjects (both as defined below) may be transferred from the Data Controller to the Data Processor. This Annexure is intended to govern such transfers.

2. DEFINITIONS

For the purposes of this Data Processing Agreement (Hereinafter referred to as "DPA")

a. **"EU"** means the European Union;
b. **"EEA"** means the European Economic Area;
c. **"GDPR"** means General Data Protection Regulation in EU Law on data protection and privacy for all individuals within the EU and EEA, also addressing the export of personal data outside the EU and EEA areas;
d. **"Supervisory Authority"** (according to Article 51 of GDPR) means an independent public authority responsible for monitoring the application of GDPR in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the union;
e. "**Applicable Data Protection Law"** means any Data Protection Law including GDPR and Pakistani Law which may apply to the terms and conditions of this Annexure and which may vary from time to time;
f. **"Working Days"** shall mean Monday to Friday from 9:00 am till 5:00 pm in Pakistan.
g. **"Data Controller"** means the natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of processing personal data, where the purposes and means of such processing are determined by Union or Member State Law, the controller or the specific criteria for its nomination may be provided for by Union of Member State Law;
h. **"Data Processor"** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
i. **"Data Subject"** means an identified or identifiable natural person who is the subject of Personal Data;
j. **"Recipient"** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
k. **"Third party"** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.
l. **"Personal Data"** means any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identified or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
m. **"Prompt Notice"** shall mean Twenty Four (24) hours unless otherwise expressly stated in this Annexure;
n. **"Special Category Data"** [according to Article 9(1) of GDPR] means any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

3. TERMS AND CONDITIONS

The Parties agree that:

a. The Data Controller and the Data Processor acknowledge that for the purposes of Applicable Data Protection Law and this DPA, Cybernet is the "Data Processor" of any personal data processed for the Data Controller in connection with the provision of the Services.

b. In the course of providing the Services to the Data Controller pursuant to this DPA, the Data Processor may process personal data as per the written instructions of the Data Controller.

c. The subject-matter of the processing of personal data by the Data Processor is the provision of the Services to the Data Controller that involves the processing of personal data.

d. The duration of processing the personal data by the Data Processor shall continue until the termination of this DPA or when there is no obligation set out in this contract any more to process data.

   This DPA shall continue for the same term as the Service Level Agreement.

e. The purpose of processing the personal data by the Data Processor under this DPA is due to the Services ordered by the Data Controller along with any other written instructions provided by the Data Controller from time to time.

f. The nature of processing the personal data by the Data Processor under this DPA is determined by and limited to the requirements for the provision of the Services ordered by the Data Controller and include compute, storage etc.

g. The Data Processor shall process Personal Data it receives from the Data Controller only for the purposes of carrying out its obligations arising under this DPA and for no other purpose except with the express written consent of the Data Controller.

h. The Data Controller shall provide written instructions to the Data Processor to process the Personal Data in any manner that may reasonably be required in order for the Data Processor to carry out the processing in compliance with this DPA and in compliance with Applicable Data Protection Law.

i. The Data Controller shall refrain from providing instructions which are not in accordance with applicable laws including Applicable Data Protection Law, and, in the event that such instructions are given, the Data Processor is entitled to resist carrying out such instructions.

j. The details of the transfer and of the Personal Data are specified in Schedule 1 of this Annexure. The parties agree that Schedule 1 may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency. The parties may execute additional annexes/schedules to cover additional transfers, or may include multiple transfers in Schedule 1, which will be submitted to the Supervisory Authority where required and applicable.

k. The confidentiality and non-disclosure rights and obligations of the parties with respect to each other under the Clause 3(k) of this DPA shall survive any termination of the DPA.

4. REGULATORY COMPLIANCE

To the extent required by Applicable Law or Regulation:

a. The Data Processor will comply with all Applicable Data Protection Laws and Regulations binding upon it in the performance of the DPA.

b. The Data Processor will cooperate, on request, with the Supervisory Authority in the performance of its tasks.

c. The Data Controller, its auditors and the Supervisory Authority will have exclusive access to the Data Processor's business premises by providing reasonable notice of ten (10) working days in accordance with the Right of Audit mentioned in this DPA Agreement;

d. The Supervisory Authority upon reasonable notice of **ten (10)** working days shall have the right of access to the Data Processor's business premises for purposes of this Clause 4(b) of this DPA; and

e. The Data Processor will give prompt notice to the Data Controller of any development that may have a material impact on the Data Processor's ability to perform services effectively under this Agreement and in compliance with applicable laws and regulatory requirements.

5. OBLIGATIONS OF THE DATA CONTROLLER

The Data Controller warrants and undertakes that:

a. The Personal Data has been collected, processed and transferred in accordance with all the Applicable Data Protection Laws and Regulations.

b. It has used reasonable efforts to determine that the Data Processor is able to satisfy its legal obligations under this DPA.

c. It has instructed and throughout the duration of the personal data processing services will provide written instructions to the Data Processor to process the personal data transferred only on the Data Controller's behalf and in accordance with the Applicable Data Protection Law.

d. It will comply with all Applicable Data Protection Laws and Regulations binding on it in the performance of this DPA.

e. To the extent required by Applicable Data Protection Law or Regulation, it will cooperate, on request, with the Supervisory Authority in the performance of its tasks.

f. It will respond to, as required by the Applicable Data Protection Law, enquiries from Data Subjects and the Supervisory Authority concerning processing of the Personal Data by the Data Controller, unless the parties have agreed that the Data Processor will so respond, in which case the Data Controller will still respond to the extent reasonably possible and with the information reasonably available to it if the Data Processor is unwilling or unable to respond.

g. The Data Controller agrees that an unsuccessful Personal Data Breach will not be subject to the Data Processor's obligation of Personal Data breach notification under the Clause 6(o) of this DPA. An unsuccessful Personal Data Breach is one that results in no unauthorized access to the Data Controller's Personal Data or to any of AWS's equipment or facilities storing the Data Controller's Personal Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents.

h. The Data Controller agrees that the Data Processor's obligation to report or respond to a Personal Data Breach under the Clause 6(p) of this DPA is not and will not be construed as an acknowledgement by the Data Processor of any fault or liability of the Data Processor with respect to the Personal Data breach.

6. OBLIGATIONS OF THE DATA PROCESSOR

The Data Processor warrants and undertakes that:

a. It will comply with all applicable laws and regulations including Applicable Data Protection Law in its performance under this DPA.

b. It will only process the Personal Data on the written instructions of the Data Controller directly relevant to the Scope under this DPA.

c. It will not transfer Personal Data to a Third Country or an international organization without the prior written approval of the Data Controller and only then once the transfer to the

Third Country has been legitimized and the Data Controller and the Data Processor are satisfied that an adequate Data Protection regime exists in the Third Country.

d. It will not transfer Personal Data to a Third Country or an international organization unless required to do so by Applicable Law to which the Data Processor is subject to. In such a case, the Data Processor will first attempt to redirect the Governmental Body to request that data directly from the Data Controller. As part of this effort, the Data Processor may provide the Data Controller's basic contact information to that Governmental Body. If compelled to disclose the Data Controller's Personal Data to a Governmental Body, then the Data Processor will inform the Data controller of the legal requirement before processing, unless the law prohibits such information on important grounds of public interest.

e. It will not appoint sub-processors to process the Personal Data on its behalf without the prior written approval of the Data Controller.

f. Once approved by the Data Controllers, the Data Processor will ensure that its sub-processors process the Personal Data only on the instructions of the Data Processor. Furthermore, the Data Processor will then put in place a legal agreement in writing to govern the sub-processing.

g. It will have in place appropriate technical and organizational measures and all measures pursuant to Applicable Data Protection Law to protect the confidentiality of the Personal Data and to protect the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

h. It will assist the Data Controller by appropriate technical and organizational measures, whenever reasonably required and applicable, in so far as possible, to fulfil the Data Controller's obligation to respond to requests for exercising the Data Subject's rights in accordance with the Clause 8 "Data Subject's Rights" of this DPA.

i. It will obtain guarantees from any sub-processors processing the Personal Data, that they will have in place appropriate technical and organizational measures, and all measures pursuant to Applicable Data Protection Law to protect the confidentiality of the Personal Data and to protect the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

j. It will have in place procedures so that any individual party it authorizes to have access to the Personal Data, including employees of the Data Processor, will respect and maintain the confidentiality and security of the Personal Data. Any person acting under the authority of the Data Processor shall be obligated to process the Personal Data only on instructions from the Data Processor. This provision does not apply to persons authorized or required by Applicable Law or Regulation to have access to the Personal Data.

k. It will not disclose any Personal Data to a third party in any circumstances other than at the specific written request or consent of the Data Controller Data Controller, unless such disclosure is necessary in order to fulfil the obligations of the Services Agreement, or is required by Applicable Law or Regulation.

l. If the Data Processor receives any request for information by any Governmental Body or the Supervisory Authority, it will first attempt to redirect the Governmental Body to request that data directly from the Data Controller. As part of this effort, the Data Processor may provide the Data Controller's basic contact information to that Governmental Body. If compelled to disclose the Data Controller's Personal Data to a Governmental Body, it will notify the Data Controller of such request before processing, unless such notification is prohibited by the Applicable Law or Regulation.

m. It will notify the Data Controller of any complaint, notice or communication received which relates directly or indirectly to the processing of the Personal Data, or other connected activities, or which relates directly or indirectly to the compliance of the Data

Processor and/or the Data Controller with relevant Applicable Law including Applicable Data Protection Law.

n. The Data Processor has provided the Data Controller with the controls to retrieve, move or delete the Personal Data. The Data Controller is able to use these controls until the termination of the Service Agreement. The Data Controller will delete all the data within **Ten (10)** working days upon the termination of the Service Agreement, once the notice period is served and the receipt of termination is acknowledged.

o. The Data Processor will delete all Personal data of the Data Controller within **Ten (10)** working days once the timeline mentioned in Clause 6(n) of this DPA has lapsed. The only exception to the Clause 6(o) of this DPA shall be where the Data Processor shall have a legitimate reason, which is confirmed by the Data Controller, to continue to process particular data or where it is legally required to maintain data records.

p. It will notify the Data Controller of a Personal Data breach without undue delay after becoming aware of the Personal Data Breach. The Data Processor will take reasonable steps to mitigate the effects and to minimise any damage resulting from the Personal Data breach.

q. The Data Processor will assist the Data Controller in pursuant to any personal data breach notifications that the Data Controller is obligated to make under the Applicable Data Protection Law or Regulation, taking into account the nature and scope of the Services, the information available to the Data Processor, and any restrictions on disclosing the information, such as confidentiality.

r. The Data Processor will assist the Data Controller in complying with the Data Controller's obligations in respect of data protection impact assessments and prior consultation pursuant to the Applicable Data Protection Law or Regulation, taking into account the nature and scope of the Services, the information available to the Data Processor, and any restrictions on disclosing the information, such as confidentiality.

s. Without prejudice to other legal provisions concerning the Data Subject's right to compensation and the liability of the parties generally, as well as legal provisions concerning fines and penalties, the Data Processor will carry liability in the instance where it or its sub-processor is found to have infringed the obligations of the applicable law including the Applicable Data Protection Law specifically directed to the Data Processors, through his processing of the Personal Data. The Data Processor will be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

t. It has no reason to believe, at the time of entering into this DPA, of the existence of any reason that would have a substantial adverse effect on the guarantees provided for under this Agreement, and it will inform the Data Controller (which will pass such notification on to the Supervisory Authority where required) if it becomes aware of any such reason.

u. It will process the Personal Data for purposes described in Schedule 1, and has the legal authority to give the warranties and fulfil the undertakings set out in this DPA.

v. It will identify to the Data Controller a contact person within its organization authorized to respond to enquiries concerning processing of the Personal Data, and will cooperate in good faith as required by the Applicable Data Protection Law, with the Data Controller, the Data Subject and the Supervisory Authority concerning all such enquiries within a reasonable time period during working hours.

w. It will be capable of demonstrating compliance to the obligations specifically directed to the Data Processors under Applicable Data Protection law.

7. RIGHT OF AUDIT

a. Upon reasonable request of the Data Controller, the Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with the obligations laid down in the Applicable Data Protection Law or Regulation and act as a supporting hand by contributing to audits, including inspections, conducted by the Data

Controller or another independent auditor mandated by the Data Controller, directly relevant and limited to the scope of the Services and this DPA.

b. Audits or inspections at the Data Processor's premises must be carried out without any avoidable or significant interruptions or disturbances to the operation of its business. These inspections shall be carried out after appropriate advance notice of **Ten (10)** working days and during the Data Processor's business hours on working days, and not more frequently than once every **Twelve (12)** months. The Data Controller shall ensure that its personnel conducting such audits are subject to adequate secrecy obligations. If the Data Processor provides evidence of the agreed data protection obligations being correctly implemented, any inspections shall be limited to samples.

c. The Data Controller is entitled to appoint a third party independent auditor to inspect the Data Processor's compliance with this DPA and the applicable data protection legislation required to determine the truthfulness and completeness of the statements submitted by the Data Processor under this DPA. The Data Controller shall bear any and all cost of the audit. Upon security audits performed by an external auditor, the Data Controller shall provide the Data Processor with a copy of the audit report.

d. The auditor appointed by the Data Controller under Clause 7(c) of this DPA must have the required professional qualifications and bound by a duty of confidentiality, must not be a competitor of the Data Processor and must be reasonably acceptable to the Data Processor.

8. DATA SUBJECT'S RIGHTS

a. The Data Processor will assist the Data Controller by appropriate technical and organisational measures, whenever reasonably required and applicable, in so far as possible, to fulfil the Data Controller's obligation to respond to requests for exercising the Data Subject's rights to access, correct and/or erase their Personal Data and the Data Subject's rights as provided under Applicable Data Protection Law.

b. The Data Processor has provided the Data Controller with the controls and functionalities through the Services, that the Data Controller may use to retrieve, correct, delete or restrict the Personal Data. Without prejudice to Clause 8(a) of this DPA, the Data Controller may use these controls as technical and organisational measures to assist it in connection with its obligations under the Applicable Data Protection Law relating to responding to requests from the Data Subjects.

9. LIABILITY AND INDEMNITY

a. The Data Processor will not be liable for any claim brought by a Data Subject arising from any action by the Data Processor to the extent that such action resulted directly from the Data Controller's instructions.

b. Except as provided for in Clause 9(a) of this DPA, the Data Processor shall indemnify the Data Controller for any monetary fine or penalty imposed on the Data Controller under the Applicable Data Protection Law that results from the Data Processor's breach of its obligations under this DPA, provided the Data Controller has provided the Data Processor with the particulars of that breach. The Data Processor will be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage or the beach.

c. In the event that any claim is brought against the Data Controller by a Data Subject arising from any action by the Data Processor, to the extent that such action did not result directly from the Data Controller's instructions, the Data Processor shall indemnify and keep indemnified and defend at its own expense the Data Controller against all costs, claims, damages or expenses incurred by the Data Controller or for which the Data Controller may become liable due to any failure by the Data Processor or its directors, officers, employees, agents or contractors to comply with any of its obligations under this DPA. The Data Processor will be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

d. In the event that any claim is brought against the Data Processor by a Data Subject arising from any action or omission by the Data Processor to the extent that such action or omission resulted directly from the Data Controller's instructions, the Data Controller shall indemnify and keep indemnified and defend at its own expense the Data Processor against all costs, claims, damages or expenses incurred by the Data Processor for which the Data Processor may become liable due to any failure by the Data Controller or its directors, officers, employees, agents or contractors to comply with any of its obligations under this Agreement.

e. The Data Controller and the Data Processor will provide each other with evidence of financial resources to confirm it has sufficient such resources to fulfil its responsibilities under Clause 9(c) and 9(d) of this DPA as appropriate (which may include proof of insurance cover and/or declaration(s) pertaining to annual turnover).

10. RESOLUTION OF DISPUTES WITH DATA SUBJECTS OR THE SUPERVISORY AUTHORITY

a. In the event of a dispute or claim brought by a Data Subject or the Supervisory Authority under the Applicable Data Protection Law, concerning the processing of the Personal Data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably within a reasonable period of time.

b. The parties agree to respond to any generally available non-binding mediation procedure initiated by a Data Subject or by the Supervisory Authority under the Applicable Data Protection Law. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

c. Each party shall abide by a decision of the Supervisory Authority which is final and against which no further appeal is possible.

d. Clauses 10(a), 10(b) and 10(c) of this DPA shall be applicable to cases that fall under this Data Processing Agreement only.

11. TERMINATION

a. In the event that either the Data Processor or the Data Controller is in breach of its obligations under this DPA, then either the Data Processor or the Data Controller may temporarily suspend the transfer of Personal Data until the breach is repaired or the DPA is terminated.

b. In the event that:

   i. the transfer of Personal Data to the Data Processor has been temporarily suspended by the Data Controller for longer than one month pursuant to Clause 11(a) of this DPA;

   ii. compliance by the Data Controller with this DPA would put it in breach of its legal or regulatory obligations in the country of import;

   iii. the Data Processor or Data Controller are in substantial or persistent breach of any warranties or undertakings given by them it under this DPA;

   iv. a final decision against which no further appeal is possible of a competent court or of the Supervisory Authority rules that there has been a breach of this DPA by the Data Controller or the Data Processor; or

   v. a petition is presented for the administration or winding up of the Data Controller, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the Data Processor is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs, then the Data Controller, without prejudice to any other rights which it may have against the Data Processor, shall be entitled to terminate this DPA in which case the Supervisory Authority shall be informed where required and applicable.

c. The Parties agree that the termination of this DPA at any time, in any circumstances and for whatever reason (except for termination under Clause 11(b)) does not exempt them from the obligations and/or conditions under this DPA with regards to the Personal Data Transfer.

12. VARIATION OF THIS AGREEMENT

The Parties may not modify this DPA except to update any information in Schedule 1, in which case they will inform the respective authorities where required and applicable. This does not preclude the Parties from adding additional commercial clauses where required and does not affect the Services Agreement between the Data Controller and the Data Processor. In cases where any conflict arises in the interpretation of these agreements, this DPA shall take precedence.

SCHEDULE 1 – DESCRIPTION OF THE TRANSFER

Data Controller:

The Data Controller for the purpose of this DPA is ["*Customer Name*"].

Data Processor:

The Data Processor for the purpose of this DPA is "Cybernet".

Categories of Data Subjects

The Data Subjects include all those natural persons whose Personal Data are transferred by the Data Controller to the Data Processor for processing under this DPA. These Data Subjects may include the customers, employees, suppliers, and end-users of the Data Controller.

Purpose of the Data Transfer/Data Processing

The purpose of the Data Transfer or the Data Processing is defined in the Clause 3(f) under the Terms and Conditions section of this DPA.

Type of Personal Data

The type of Personal Data include all the Personal Data provided by the Data Controller to the Data Processor through the use of the Services under the Data Controller's Cloud service account at Cybernet.