t +27 (0) 10 140 5000 e sales@saicom.io w saicom.io

PRODUCT ANNEXURE - ANYCLOUD - SAICOM PRIVATE CLOUD

1. INTRODUCTION

This Product Annexure sets out the legal framework for the provision and use of Virtual Hosting Services provided by the Supplier. This Product Annexure is subject to and must be read in conjunction with the Supplier terms and conditions located at https://saicom.io/. The nomenclature used in the Agreement shall apply to this Product Annexure.

2. DEFINITIONS

2.1. **Saicom Private Cloud** - an end-to-end offering of datacenter and infrastructure services for hosting customer servers, applications and data on Saicom hosted infrastructure at the Teraco Datacenter Facilities in Isando, Johannesburg in South Africa.

2.2. **AnyCloud Portal** - A Hybrid Multi-Cloud management portal, to manage and provision servers and applications on the Saicom Private Cloud or other supported public cloud platforms.

2.3. **The Customer's Content** - Content that The Customer or any End User transfers to us for processing, storage or hosting by the Services in connection with The Customer's Supplier account and any computational results that The Customer or any End User derive from the foregoing through their use of the Services. For example, The Customer's Content includes Content that The Customer or any End User stores in the supplier Storage Service. The Customer's Content does not include Account Information.

2.4. **API** - Application Program Interface.

3. SERVICE OFFERING

3.1. The Supplier will provide the service for the monthly or hourly fees agreed in any proposals sent and signed off by both parties, as per the following items:

3.1.1. vCPU's (per single core)

3.1.2. RAM (per GB of Memory)

3.1.3. Various performance tiers of storage (per GB of storage)

3.1.4. Hybrid Multi-cloud Management Platform (per instance - as below)

3.1.4.1. All instances hosted on the Saicom Private Cloud are exempt from this per instance cost. Only workloads managed through the AnyCloud Portal on any other configured 3rd party platform (on-premises, hosted, or public clouds) would be subject to this per instance cost.

3.1.4.2. An Instance is defined as a set of containers or virtual machines that can correlate to a single horizontally scalable entity or a service suite e.g. Apache web farm

3.2. Any quantity change based on The Customer's usage per month and will be billed according to the Saicom cloud platform usage reporting tools.

3.3. A price renegotiation with an agreed proposal must be signed off by both parties.

4. THE SUPPLIER'S OBLIGATIONS AND SERVICE RESPONSIBILITIES

4.1. The Supplier will be responsible for providing infrastructure hosting services for the Customer's servers in the secure and highly available datacenter facilities, including the provisioning of:

4.1.1. Highly available and redundant server, storage, network and firewall infrastructure with a 99% uptime service level for unscheduled downtime 24/7/365, hosted on supplier Infrastructure at the Teraco Johannesburg (Isando) datacenter in South Africa;

4.1.2. Access to at least two internet service providers at our datacenters;

4.1.3. Dedicated public IP addresses required for The Customer's hosted servers, 1 per server;

4.1.4. Dedicated internal virtual IP address network and VLAN segmentation on our hosted network, including the Customer's own dedicated tenant creation on our cloud management platform with role-based security capabilities;

4.1.5. Redundant storage for The Customer's hosted data storage infrastructure backed by vendor 4-hour mission critical support;

4.1.6. Shared compute (CPU & Memory) for The Customer's hosted virtual servers;

4.1.7. Failover of The Customer's virtual servers to other available infrastructure hosted in the same datacenter in the event that The Supplier experiences a hardware malfunction;

4.1.8. 24/7/365 maintenance, monitoring and support to ensure our hosted infrastructure is functional and can provide the required resources for The Customer's servers and application services to be online from a compute, storage, network and firewall perspective;

4.1.9. Any approved change control changes the Customer request to The Customer's hosted server from a virtual hardware perspective, for example changes to CPU, Memory, Disk, Network etc;

4.1.10. Monitoring on the usage and trending of The Customer's hosted virtual servers;

4.2. Reporting on the usage and trending of The Customer's hosted virtual servers is available upon request. This reporting would include:

4.2.1. Local Virtual Server CPU Usage

4.2.2. Local Virtual Memory Usage

4.2.3. Local Virtual Server Disk Capacity

4.2.4. Hosted Disk Capacities

4.2.5. Hosted infrastructure Availability & Uptime

4.3. The Supplier would also provide:

4.3.1. Customer management access and/or API access to The Customer's hosted Servers via:

4.3.1.1. AnyCloud Portal (https://anycloud.saicom.io);

4.3.1.2. Remote Access (Remote Desktop Protocol RDP, Secure Shell SSH, Web Console);

4.3.2. Approved firewall or network port changes on our firewall infrastructure to support public access to the Customer's hosted servers. Note this would need to be agreed to by both Saicom Cloud Hosting and the Customer and in order to not compromise the security of the Customer's servers and our infrastructure.

4.3.3. Security monitoring, intrusion detection and auditing of our firewall and network infrastructure, including our management servers and processes and procedures;

4.3.4. Patch Management will be automated for the Supplier infrastructure based on our patch management policy.

4.4. The supplier will ensure the Customer's hosted servers will have a dedicated internal virtual network with a dedicated VLAN and are protected by a highly available firewall configuration.

4.5. No default usernames and passwords are used for any hardware or software supplied by the Supplier.

4.6. The hosted datacenter is permanently monitored and sits behind configured hardware firewalls.

4.7. Any local security accounts required for the service will be unique to each person using the system.

4.8. In the event The Supplier cannot provide the cloud services to The Customer any longer for whatever reason, The Supplier will provide The Customer with The Customer's data and servers stored on our infrastructure via an agreed upon method.

5. THE CUSTOMER'S RESPONSIBILITIES

5.1. To access the Services, the Customer must have an approved AnyCloud Portal account associated with a valid email and business address and a valid form of payment for the services.

5.2. Except to the extent caused by our breach of this Agreement, (a) The Customer is responsible for all activities that occur under the Customer's account, regardless of whether the activities are authorised by The Customer or undertaken by The Customer, the Customer's employees or a third party (including The Customer's contractors, agents or End Users), and (b) the supplier and our affiliates are not responsible for unauthorized access to The Customer's account.

5.3. The Customer will ensure that the Customer's Content and the Customer's End Users' use of the Customer's Content or the Service will not violate any applicable law. The customer is solely responsible for the development, content, operation, maintenance, and use of the Customer's Content.

5.4. The Customer is responsible for properly configuring and using the Service and otherwise taking appropriate action to secure, protect and backup the Customer's accounts and the Customer's Content in a manner that will provide appropriate security and protection, which might include use of encryption and two factor authentication to protect the Customer's Content from unauthorized access and routinely archiving the Customer's Content.

5.5. Nothing contained in this Product Annexure will be seen as a representation that any back-ups of data the Supplier has implemented will be successful or in any way will assist with disaster recovery.

5.6. The Customer's account log-in credentials and private keys generated by the Service are for the Customer's internal use only and the Customer will not sell, transfer or sublicense them to any other entity or person, except that the Customer may disclose the Customer's private key to the Customer's agents and subcontractors performing work on the Customer's behalf.

5.7. The Customer will be deemed to have taken any action that the Customer permits, assists or facilitates any person or entity to take related to this Product Annexure, the Customer's Content or use of the Service Offerings. The Customer is responsible for End Users' use of the Customer's Content and the Service Offerings. The Customer will ensure that all End Users comply with the Customer's obligations under the Contract Documents and that the terms of the Customer's agreement with each End User are consistent with the Contract Documents. If the Customer becomes aware of any violation of the Customer's obligations under the Contract Documents caused by an End User, the Customer will immediately suspend access to the Customer's Content and the Service Offerings by such End User. The Supplier does not provide any support or services to End Users unless the Supplier has a separate agreement with the Customer or an End User obligating it to provide such support or services.

5.8. The Customer will allow the Supplier to install monitoring, utility or diagnostic programmes to assist the Supplier in providing the services only. These tools will not expose any of the Customer's Content in any way.

5.9. If required, obtaining the consent of the owner of software to allow the Supplier to use the source code of the software or such part of the source code as may be necessary to enable the Supplier to diagnose and assist in the resolution of support requests.

5.10. The Customer is responsible for ensuring installation, automation and maintenance of any required operating system security patches, anti-virus, anti-spam, intrusion detection, ransomware and spyware protection on the Customer's hosted servers and applications.

5.11. The Customer is responsible for ensuring the that local firewall on the Customer's hosted servers is configured correctly to protect the Customer's applications and data.

5.12. The Customer agrees to only make use of properly licensed third party software in connection with its use of the Services and agrees to indemnify and hold the Supplier and any of its members, representatives, officers or employees harmless against all losses, damages, liability, costs and expenses, including reasonable attorney fees, suffered or incurred by them as a result of any third party claims relating to its involvement in any copyright infringement or alleged copyright infringement.

6. MICROSOFT LICENSING

6.1. With the Service Provider Licence Agreement (SPLA), the Supplier can licence Microsoft products and use these licensed products ("products") to provide software services and hosted applications to our Customers.

6.2. Software services are services that the Supplier provides to Customers that make Microsoft products available and that display, run, access, or otherwise interact with Microsoft products. The Supplier can provide these services from one or more data centres via the Internet, a telephony network, or a private network on a rental, subscription, or services basis, whether or not our customers receive a fee.

6.3. Software services exclude installing a Microsoft product directly on any device to permit a Customer to interact with the Microsoft product.

6.4. Should the Customer be utilising the Supplier's dedicated Virtual Machines, Virtual Data Centre, or Microsoft Azure platform, Customer's do not have to purchase Microsoft licensing from the Supplier but all customers must sign and adhere to the 'Microsoft license mobility' agreement, ensuring that both the Supplier and Customer are compliant with Microsoft licensing rules.

6.5. Even if the Customer does not sign the Microsoft mobility agreement the Customer agrees that the sole responsibility of adhering to Microsoft's licensing rules is the Customer's.

6.6. The Customer gives both the Supplier and/or Microsoft the right to audit the Customer's environment at any time to ensure that the customers licensing is compliant at all times.

7. HARDWARE AND SOFTWARE

7.1. The Supplier will provide sufficient hardware and software licensing to perform the required services. If:

7.1.1. If The Customer purchase any of the hardware or software licensing from the supplier, The Customer will be subject to our standard terms of sale;

7.1.2. If the Customer leases any of the hardware from the Supplier, the provisions of the Agreement and the Supplier's standard lease agreement shall govern the lease of such hardware; and

7.1.3. If the Customer procures any of the hardware or software licensing from a third-party supplier, the Customer will ensure that the hardware and software meet the Suppliers minimum specifications and are configured in accordance with the Supplier's requirements.

8. ROUTINE SERVICE MAINTENANCE TASKS

8.1. The supplier will:

8.1.1. Maintain and support the Service infrastructure via regular and planned maintenance schedules, ensuring the hardware and software is functioning optimally and securely. This may require scheduled maintenance for updates and required changes to the infrastructure when or where necessary;

8.1.2. Follow documented and approved processes via our IT service management tools to support and maintain the Service;

8.1.3. Provide The Customer with adequate notification of any critical changes that need to be made to the Service that would impact Service availability;

8.1.4. Maintain up to date documentation of the Service configurations;

8.1.5. Make changes to hosted virtual servers on The Customer's request and approval, when or where necessary;

9. MONITORING

9.1. The Supplier will provide monitoring software that can notify on:

9.1.1. Hardware or software failures relating to our hosted services;

9.1.2. Hardware infrastructure and related software failures; and

9.1.3. ISP wide area network connectivity and bandwidth issues;

10. DISTRIBUTED DENIAL OF SERVICE (DDOS)

10.1. If the Server becomes the target or source of any form of Denial of Service Attack the Supplier may disconnect the Server from the network.

11. ILLEGAL ACTIVITY

11.1. The Supplier has the right to shut down any service where it reasonably believes any illegal activity is being performed on or via such service.

12. NOTIFICATION OF FAILURES

12.1. The Supplier personnel will:

12.1.1. assess any infrastructure failures related to the Customer's hosted servers;

12.1.2. advise the Customer of the status and expected progress in the resolution of all failures that are referred to a third-party supplier.

13. DATA SECURITY AND PRIVACY

13.1. Without limiting the Supplier obligations for security in clause 4 or the Customer's in clause 5, the Supplier will implement reasonable and appropriate measures designed to help the Customer secure the Customer's Content against accidental or unlawful loss, access or disclosure.

13.2. The Customer consents to the storage of the Customer's Content in, and transfer of the Customer's Content into, the Saicom cloud infrastructure located inside the South African region hosted at the Teraco datacenters. The Supplier will not access or use the Customer's Content except as necessary to maintain or provide the Services, or as necessary to comply with applicable law, a binding order of a governmental body. The Supplier will not move or store the Customer's Content from the South African region without the Customer's express consent.

13.3. Notwithstanding that the Customer's services are hosted in the Supplier's cloud, Customers must take security precautions to protect its virtual environment. The Customer acknowledges that the Supplier will not be responsible for any damage suffered by the Customer as a result of third-party's unauthorized access and damage caused to the Customer's environment.

13.4. It is the Customer's responsibility to ensure that scripts/programs installed under their account are secure and permissions of directories are set properly, regardless of installation method. Users are ultimately responsible for all actions taken under their account. This includes the compromise of credentials such as username and password. It is required that Customers use a secure password.

13.5. Unless specifically contracted as a service between the Supplier and the Customer, patching, updates and firewalling of the Customer's hosting environment is the responsibility of the Customer and the Supplier does not take any responsibility for any breaches.

14. SPECIFICATION AMENDMENTS

14.1. If a party, at any stage, requires any amendment to the Service specifications, it will submit a written change request to the other party, setting out:

14.1.1. the nature of the desired changes;

14.1.2. the reason for the changes; and

14.1.3. the effect of the changes on the deliverables;

14.2. If the proposal is made by:

14.2.1. The Customer, The Supplier will investigate the likely impact of any proposed changes and will provide The Customer with a written response through change control approval;

14.2.2. The Supplier, The Supplier will detail the likely impact of any proposed changes and will provide The Customer with a written response through change control approval;

14.3. Until any changes have been mutually agreed in writing, the parties will continue to perform their respective obligations under this order.

15. OWNERSHIP OF DELIVERABLES

15.1. All right, title and interest, including all rights under all copyright, patent and other intellectual property laws, in and to the deliverables will vest in the Supplier.

15.2. During the Term, each party grants to the other party (and their contractors as necessary) a temporary, non-exclusive license to use, reproduce and modify any of its existing material provided to the other party solely for the performance of the services. The Customer's license to Supplier existing material is conditioned upon the Customer's compliance with the Contract Documents.

16. SUPPORT

16.1. The Supplier will provide a help desk 24/7/365 for service requests related to the Services.

16.2. The Customer is primarily responsible for the Customer's hosted server application environment functionality. The Customer must resolve and diagnose application errors running inside the Customer's hosted server.

16.3. The Customer will, before logging a service request with the Supplier, thoroughly research any problem encountered and will make sure that all the details relating to the problem are available to disclose to the Supplier service desk;

16.4. Only the Customer's designated personnel as listed in the information schedule may make support requests to the service desk.

16.5. The Customer's support resource will place a service request on the Supplier service desk, stating the necessary information. The service request will be made in writing, either via email or a telephone call that is confirmed in writing.

16.6. Upon receipt of the service request, the Supplier service desk will evaluate the service request and communicate its appraisal to the Customer. If a service request does not fall within the scope of the retained services, the Supplier shall notify the Customer of same and the request will be added to the Customer's wish list and dealt with in a separate order.

16.7. Once a service request has been resolved, the Supplier service desk will inform the Customer's support resource. The Customer's support resource will, within a reasonable period thereafter (having regard to when the problem would reasonably be detected by the Customer again) inform the Supplier through its help desk whether the correction was satisfactory to the Customer or not. If no notice is received, then the problem will be deemed to have been corrected to the Customer's satisfaction and the service request ticket will be closed.

17. EXCLUDED SERVICES

17.1. The Supplier will not provide the Customer with:

17.1.1. Any application support or maintenance running inside the Customer's hosted server other than that specified in this Product Annexure or the Customers Proposal, this includes operating system support, patching and security management;

17.1.2. Business continuity and disaster recovery services;

17.1.3. Anything outside of what is listed as part of our service obligations and responsibilities to the Customer.

18. WARRANTIES AND DISCLAIMERS

18.1. The Customer is responsible for the integrity of the Customer's Content stored inside the Customer's hosted servers.

18.2. The Supplier will not be responsible for:

18.2.1. an error or fault caused by third party hardware or software used in conjunction with the Products or Services, unless expressly agreed to in the Customer’s Order;

18.2.2. any defects or errors resulting from any modifications to the Products or Services made by any person other than the Supplier personnel or appointed representatives.

18.2.3. The Customer's inappropriate use of the Service or operator error.

18.2.4. any fault in any third-party software or hardware used in conjunction with the Service Offerings, unless expressly stipulated in the Customer’s Order;

18.2.5. services carried out at the Customer's request, which the Supplier finds to arise from the incorrect reporting of a defect or error; and

18.2.6. the effects, problems or errors caused to the Products and Services as a result of the Customer's failure to maintain the Customer's server operating system and application system correctly or to protect against viruses, ransomware or malware.

18.3. The Supplier does not warrant that any bespoke task the Supplier undertakes for the Customer will be error free.

19. THE CUSTOMERS FAILURE

19.1. If the Customer fails to comply with the Customer's obligations for a period in excess of seven calendar days after receiving a written request from the Supplier for the Customer to do so, the failure will constitute a material breach the Customer. In addition to any remedies the Supplier may have arising out of the breach, the Supplier will be excused from meeting the service levels for as long as the Customer fails to comply with the Customer's obligations.

20. CANCELLATION

20.1. For convenience, the services used by the Customer may be cancelled for any or no reason by either party with a preceding calendar month’s notice.

20.2. After the calendar month period the Customer’s Account will be ended and the Customer will no longer have access to the AnyCloud portal.

20.3. If the workload has not been successfully migrated off the Saicom Private Cloud, a powered down copy of the workloads will be made available for download for a further calendar month, afterwhich all workloads and any other information or data related with the account will be deleted from the Supplier’s servers.

END OF ANNEXURE