AKAZA MULTI CLOUD SERVICE AGREEMENT

IT IS HEREBY AGREED BY AND BETWEEN THE CUSTOMER AND SLT AS FOLLOWS:-

1. Definitions

1.1 "**Service**" shall mean the provision of the virtual hosting services called Akaza Multi Cloud Hosting Service and related services, through the Platform selected by the Customer as morefully described in the **Annex 1** hereto.

1.2 "**Site**" shall mean the location/s where the hosting infrastructure including SLT equipment are located as detailed under **Annex 2.**

1.3 "**Customer Content"** or **"Customer Data"** shall mean any data hosted by the Customer, including all text, sound, video, or image files, and software (including personally identifiable information and machine images) on the Platform.

1.4 **"Platform"** means the cloud based software program selected by the Customer as detailed under Annex 1 to host Customer Content in obtaining the Services.

1.5 Words imparting the singular shall include the plural and vice versa and words imparting one gender shall include the other gender.

2. Provision and commencement of the Service

SLT shall provide the Customer with the Service selected by the Customer as detailed under Annex 1 hereto, for the period stated under Schedule hereof, for use by the Customer for any lawful purposes, subject to the due observance and performance by the Customer of the terms and conditions contained herein and the due payment by the Customer to SLT of all fees and other charges payable to SLT hereunder. Service is subscribed/licensed for the period under the Schedule and not sold.

3. Representations and Warranties

3.1 The Customer represents and warrants that:

(a) The Customer has the power and authority to enter into and fully perform its obligations under this Agreement and to grant the rights granted in this Agreement and Entering into this Agreement does not constitute a breach by the Customer of any statutory, contractual or fiduciary obligations ;

(b) The Customer has obtained, at the Customer's own cost, all licenses, permits, consents, approvals and intellectual property or other rights and approvals of any network/person as may be required for using the Service;

(c) The Customer Content, material, messages, Customer Data and any other data transmitted or made available through the Services does not contain material that is inaccurate or that violates any applicable law, rule or regulation;

(d) The content, material, messages and data transmitted or made available through the Services (including Customer Content) does not infringe any common law or statutory right of any person or entity, including, without limitation, any proprietary, contract, moral, privacy or publicity right, copyright, patent, trademark, trade secret, or any other third party right;

(e) That Customer owns the Customer Content or otherwise has the right to place the Customer Content on the Platform or in the use of the Service;

(f) The content, material, messages and data transmitted or made available through the Services (including Customer Content) do not contain any material that, in the Customer's good faith judgment, is obscene, threatening, malicious, defamatory, libelous, slanderous, pornographic or otherwise expose SLT to civil or criminal liability;

(g) The Customer has obtained any and all authorization(s) necessary for hypertext links from the Customer's website to other third party web sites;

(h) The Customer will not use the Services to send unsolicited e-mails, or engage in any other offensive or harassing or disturbing conduct, or conduct that unreasonably interferes with SLT's ability to manage its network facilities or provide similar Services to other customers.

3.2 In addition to any other remedies set forth in this Agreement, SLT reserves the right to immediately remove from the Customer's hosted resources, including any Virtual CPUs, Virtual RAMs, Storage, material (virtual machines or data centers which violates any of the above warranties and/or to immediately disable any Services necessary to remedy any violation or potential violation of the above warranties.

3.3 SLT represents and warrants that

(a) SLT has the legal right and authority to provide the Services

(b) SLT equipment referred under Clause 9.4 are the property of SLT.

3.4 No other Warranty.

Other than the express warranties contained in Clause 3.3 and the service availability stated in Clause 6.2 herein, all Services performed pursuant to this Agreement are performed on an "as is" basis, and Customer's use of the Services is at its own risk. SLT does not make, and hereby disclaims (further to Clause 11 herein), all other warranties, merchantability and fitness for a particular purpose. SLT does not warrant that the Services provided hereunder will be uninterrupted, error-free, or completely secure**.** SLT shall also not be liable for any loss or damage sustained by the Customer due to reason of failure, breakdown or interruption of the Service whatsoever, notwithstanding the cause of such failure, breakdown or interruption of the Service and however long it shall last. Furthermore, no reduction in rates or outage credit shall be due to the Customer in the event of such occurrences**.**

4. Fees, Payment and Billing

4.1 Customer shall pay the fees ("Fees") set forth in Annex 3, and the invoice on a monthly basis for the Services, may it be an initiation charge or monthly subscription which payment shall be made within thirty (30) days of the date of each invoice.

4.2 Late Payment.

Customer's failure to pay any Fees upon due dates shall be a material breach of this Agreement, and SLT may, in addition to any rights available to it under the terms herein or law or in equity, do any or all of the following;

(i) charge interest at the rate of two per centum (2%) per month on the Fees that remain unpaid up to the date of complete payment;

(ii) terminate the Agreement if the over due payment is not settled within a further 30 days notice period given as grace in addition to the 30 days provided for fee settlement;

(iii) require future payments hereunder to be made in advance prior to delivery of Services.

Any suspension or termination of Services will not relieve the Customer from the obligation to pay the Fees due for the Services already rendered. In event of collection enforcement, Customer shall be liable to pay any costs associated with such collection, including, but not limited to, legal costs, attorneys' fees, costs, and collection agency fees.

4.3 Default

Customer undertakes and agrees that in the event the Customer fails to perform according to this Agreement or if SLT terminates this Agreement in terms of Clause 7 herein, SLT shall be entitled to recover from the Customer all the monthly subscription stated in Annex 3 calculated over the balance period of the Agreement stated under the Schedule hereof and any outstanding payments, by way of damages and not by way of penalty in addition to any other remedies SLT may have.

4.4 Taxes.

Customer shall pay or reimburse SLT of all present or future sales, indirect, use, transfer, privilege, excise, and all other taxes and all duties, and all telecommunication levies, imposed by reason of the performance by SLT under this Agreement as stated under the invoice; excluding, however, income taxes on profits which may be levied against SLT.

4.5 Bill disputes

In the event of the Customer dispute relating to the Customer's liability to pay any such amount, the Customer shall, after making the payment, notify SLT of the said dispute. Thereupon, SLT shall examine such dispute. In the event that such a dispute is decided by SLT, in the Customer's favour, SLT shall refund to the Customer any excess amount paid by the Customer.

5. Customer Responsibilities.

5.1 Customer is responsible for all use of the Services that occurs under the Login Credentials of the Customer.

5.2 The Customer shall abide by the currently applicable Acceptable Use Policy of SLT, and the same shall be an integral part hereof. Services are subject to usage limits, including; the quantities specified in the Annex 1. Unless otherwise specified, (a) any one other than the named User, (b) a User's password shall not be shared, Any excess use shall render the Customer liable to pay for additional quantities of the applicable Services promptly upon SLT's invoicing for such excess usage in accordance with Clause 4. In the event the Service is used by the Customer for any activity that may cause change in traffic in excess of its normal usage and/or is likely to cause congestion in SLT's network, SLT shall have the right to take any action to mitigate the risk to SLT network.

5.3 Customer is solely responsible for all updates or modifications to the Customer Content during the tenure of this Agreement.

5.4 Customer shall maintain the updated software versions available from time to time as recommended by software vendors. Any vulnerability identified on software and applications need to be rectified by the Customer.

5.5 Be solely responsible for all information retrieved, stored and transmitted through the Service by the Customer.

5.6 Comply with all applicable laws and if applicable, laws of other jurisdictions, including without limitation the Sri Lanka Telecommunication Act and its amendments, and any regulations made pursuant thereto and any terms and conditions of any licenses of SLT and licenses of the Customer. Further Customer shall comply with terms and condition of this Agreement including Platform specific conditions under Annex 5 and the terms and conditions defined by software vendors from time to time and their accompanying license agreements.

5.7 Not use the Service to send messages without reasonable cause or to cause any threat, harassment, annoyance, inconvenience or anxiety to any person.

5.8 Not use the Service to send or receive any message which is offensive on moral, religious, racial or political grounds or of an abusive, indecent, obscene or menacing nature.

5.9 Take all necessary steps to ensure that no computer viruses or harmful programs are introduced and/or transmitted either through the use of an apparatus or otherwise into a telecommunication network which could be accessed through or by the use of or connected to the Service, whether that network belongs to SLT or a third party.

5.10 Comply with all notices or instructions given by SLT from time to time to the Customer in respect of the use of the Service and any infrastructure requirements needed for the provision of the Service.

5.11 Customer shall ensure that the Customer and/or the End Users of the Customer shall comply with terms and conditions of the Principal vendors or their End User License Agreements (EULA).

5.12 In the event there is a Customer involvement in the Service operation as expressly communicated by SLT, the Customer shall have the required competency for the same, in failure whereof SLT shall require the Customer to enter into a maintenance agreement for the Service operation in consultation with SLT.

5.13 In the event of service unavailability, the same shall be brought to the notice of SLT officials as in the Customer support escalation matrix under Annex 4.

5.14 Customer shall adhere to the following usage restrictions. Accordingly, the Customer shall not (a) make the Service available to, or use the Service for the benefit of, anyone other than for itself or its User, (b) sell, resell, license, sublicense, distribute, rent, lease or share with any other person the Service or generate revenue through the Service or any part of it, either for a fee or a gratification or otherwise, (c) use the Service to store or transmit abusive, indecent, obscene, of menacing nature, infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy rights, (d) use a Service to store or transmit Malicious Code, (e) interfere with or disrupt the integrity or performance of any Service or third-party data contained therein, (f) attempt to gain unauthorized access to any Service or its related systems or networks, (g) permit direct or indirect access to or use of any Service in a way that circumvents a contractual usage limit, (h) copy a Service or any part, feature, function or user interface thereof, (i) access any Service in order to build a competitive product or service, or (k) reverse engineer any Service (l) Not use the Service for any illegal or immoral activity, malicious purposes or cause harm or threat to any other person by the use of the Service.

5.15 Customer responsibilities are further detailed under the Annex 5 hereto

6 SLT Responsibilities.

SLT shall:

6.1 SLT shall make available the Service from the date morefully stated under the Schedule. The Service will be available for the customer 24x7, except for scheduled maintenance and required repairs.

6.2 SLT guarantees an overall monthly Service availability of 99.9% for all Services. Service Level Agreement under Annex 6 (Platform wise service levels when applicable) shall be adhered to by SLT.

6.3 Service downtime does not cover non iDC network/service outage which shall be covered under a separate agreement. Further, the Service levels under Annex 6 (containing all sub-annex 6 where applicable) shall not be adhered to when there is a scheduled maintenance including but not limited to Scheduled Network Maintenance, Hardware Maintenance. However, SLT will notify such scheduled maintenance in advance to the Customer. Software Maintenance requires to be done by the Customer for Customer supplied software as per Clause 5.4.

6.4 SLT responsibilities are further detailed under the Annex 5 hereto. Platform specific obligations are also detailed therein.

7 Term and Termination

7.1 Term of the Service shall be as detailed under the Schedule hereto. All Services hereunder shall be delivered during that period.

7.2 Notwithstanding anything to the contrary contained in this Agreement or any other agreements between the Parties hereto, SLT may without prejudice to any legal right or remedy which may be available to it for any breach or non-observance by the Customer of the terms and conditions herein, disconnect the Service or terminate the Service and any other services provided by SLT to the Customer, and remove and to do all such things to remove Customer Data from SLT systems/cloud as detailed under Clause 8.7 on any one of the following grounds,:

With notice to Customer if;

a) The Customer fails to pay to SLT any monies due and/or payable to SLT;
b) The Customer fails to perform or commits a breach of the Customer's obligations hereunder or is found to be in breach of the Customer's warranties and/or representations hereunder;

With immediate effect if;

a) The Customer enters into liquidation or compounds with the Customer's creditors or suffers any similar action in consequence of debt;

b) The Customer is ordered/directed to cease or suspend its business by any regulatory body;
c) If, state or any regulatory authority or governmental body have issued a direction to SLT, not to continue with the Service;
d) The Customer is, in the opinion of SLT, using the Service, for illegal or immoral activities or against the interest of public or security or criminal action has been taken or is in the process of being taken against the Customer for the use of any service which is linked or connected to the Service;
e) If the Customer's agreement with any other person or body of persons, either regulatory or otherwise, either in this country or abroad, is determined or any person whose consent is required for the effective operation of the Service withdraws such consent;

7.3 In the event the Service is terminated in terms of this Clause, SLT shall have the sole discretion in deciding whether to reconnect the Service or not.

7.4 Customer undertakes and agrees that in the event the Customer fails to perform according to this Agreement or if SLT terminates this Agreement in terms of this Clause 7, SLT shall be entitled to recover from the Customer, the monthly subscription stated in the Annex 3 hereto, calculated over the balance period stated in the Schedule hereof, imposed by way of damages and not by way of penalty, in addition to any outstanding amounts and any other remedies SLT may have. In addition, the Customer shall settled all payments in arrears.

8 Data Privacy

8.1 The Customer shall be solely responsible for Customer Content and keep SLT indemnified of its use, accuracy, Intellectual Property Rights and all third party claims on such Customer Content.

8.2 Customer is solely responsible for ensuring that the Service and its security (a) is appropriate for Customer Content and intended use by the Customer, (b) Customer has the appropriate or required certifications for Customer Content, and (c) meets all their requirements including any legal requirements that apply to them or Customer Content.

8.3 Customer is responsible for taking and maintaining appropriate steps to protect the confidentiality, integrity, and security of Customer Content and Customer Data. Those steps include (a) controlling access they provide to their Users, (b) configuring the Services appropriately, (c) ensuring the security of Customer Content and Customer Date while it is in transit to and from the Services (d) using encryption technology to protect Customer Content, and (e) backing up Customer Content.

8.4 Customer is responsible for providing any necessary notices to Users and obtaining any legally required consents from Users regarding their use of the Services.

8.5 The Customer shall, at all times, comply with its respective obligations under all applicable Data protection laws in relation to all personal Data.

8.6 In the course of providing the Services, SLT may have access to, or may come into possession of, personal information (including, any sensitive personal data and/or personally identifiable information) of Customers. The Customer understands that SLT may be required to host and/or share such personal data, Customer Data, Customer Content and confidential information with any subsidiary and/or any subcontractor and/or any principal vendor of SLT in order to provide the Services set out in this Agreement. The Customer hereby agrees and consents to such sharing, even cross borders, on the understanding that SLT takes reasonable confidentiality obligations, technical and organizational security measures to prevent any unauthorized or unlawful disclosure or processing of such information and data. Customer can access Data Protection and Privacy compliances located at www.slt.lk or at such other location as may be determined by SLT from time to time.

8.7 Customer Data Portability and Deletion - Upon any request made by the Customer within 30 days after the effective date of termination or expiration of this Agreement, SLT will make Customer Data available for the Customer to remove, export or download as reports. After that 30-day period from the termination or expiration of this Agreement, SLT will have no obligation to maintain or provide Customer Data to the Customer and will thereafter delete or destroy all copies of Customer Data in SLT systems/cloud or otherwise in SLT's possession or control, unless the retention of the same is legally required. In the event the Customer requests data migration services from SLT and SLT agrees to the same, the service rates shall be mutually agreed to by the parties.

8.8 SLT shall only store, copy or use the Customer Data to the extent necessary to perform its obligations under this Agreement and shall not disclose it to any third party other than if required to do so by a regulator or by any applicable laws or regulations.

8.9 SLT shall notify the Customer in writing within 72 hours of any confirmed or reasonably suspected breach of personal data of the Customer that is processed pursuant to this Agreement.

9. Proprietary Rights and Licenses.

9.1 Customer Content.

9.1.1 As between SLT and the Customer, the Customer shall retain all rights and interest, including, without limitation, all copyrights, trademarks, patents, trade secrets, and any other proprietary rights, in the Customer Content.

9.1.2 If SLT reasonably believe a problem with the Services may be attributable to Customer Content or to Customer use of the Services, Customer must cooperate with SLT to identify the source of the problem and to resolve the problem.

9.2 Customer hereby permits/license/consents SLT to host, copy, transmit and display Customer Data, worldwide in SLT systems/applications/cloud when providing the Service by SLT or share the same as detailed under Clause 8.6.

9.3 Monitoring.
SLT monitor and collect configuration, performance, and usage data relating to Customer use of the Services (a) to facilitate delivery of the Services (such as (i) tracking entitlements, (ii) providing support, (iii) monitoring the performance, integrity, and stability of the Services infrastructure, and (iv) preventing or addressing service or technical issues; and (b) to improve SLT products and services, and Customer experience. Customer must not interfere with that monitoring. SLT will not access Customer Content/Customer Data except if required to do so by a regulator or by any applicable laws or regulations. Such monitoring by SLT shall not discharge the Customer of its responsibilities hereunder.

9.4 SLT Equipment.
SLT retains all rights to the Services and any computer hardware, software, telecommunications or other equipment, including the Host Server, its Virtualizations Software (collectively, the "SLT Equipment") at the Site. At no time shall Customer have any ownership, property, or any other rights in, nor a claim or lien on, any of the Services or the SLT Equipment hardware and software.

10. Confidentiality

10.1 The Parties hereby undertakes that they will keep in the strictest confidence, except where disclosure is required by law, any confidential or proprietary information or intellectual property of any nature belonging to the disclosing party which may come into the possession or to the knowledge of the receiving party during its association with the disclosing party, except where the prior written consent of disclosing party is obtained.

10.2 The receiving party agrees that, if the receiving party fails to observe its obligations set forth in this Clause, the disclosing party shall be immediately entitled to injunctive and other equitable relief ordering the receiving party to specifically perform the obligations of the receiving party under this Clause. Such rights to specific performance and an injunction shall be cumulative and in addition.

11. Exclusion of Liability and Disclaimer

11.1 The Customer shall have no claim for damages consequential or otherwise or any other claim whatsoever against SLT on account of loss of revenue, business or any other basis, either for itself or for any third party, consequent to the suspension, removal, disconnection or termination of the Service provided by SLT.

11.2 SLT shall not, under any circumstances whatsoever, be liable to the Customer for any loss or damage sustained directly or indirectly by the Customer or its Customer(s), licensees or agents and others, due to the reason of the failure of the Customer to maintain its applications and operating systems in proper order, free from computer viruses or harmful programs being introduced or been let into /or transmitted either through the use of an apparatus or otherwise into a telecommunication network while the use of SLT service. SLT disclaim other warranties as stated under Clause 3.4.

12. Indemnification

The Customer shall indemnify SLT against any loss or other liabilities which may arise as a result of inter alia the Customer's negligence and/or omission and/or failure to fulfill the Customer's obligations under this Agreement, including any intellectual property rights arising out of the use of the Service, the use of the Service by the Customer for illegal or immoral purposes or for the transmission and/or introduction of harmful computer viruses or programmes into inter alia telecommunication networks, computer systems, computers and computer apparatus, any unauthorized use of the Service and the violation of any applicable laws and regulations by the Customer.

13. Force Majeure

Neither party shall be deemed in default or otherwise liable under this Agreement due to its inability to perform any of its obligations by reason of an event beyond its reasonable control including but not limited to fire, earthquake, flood, substantial snowstorm, epidemic, accident, explosion, casualty, strike, lockout, labor controversy, riot, civil disturbance, act of public enemy, embargo, war, act of God, or any municipal, or national ordinance or law, or any executive, administrative or

judicial order (which order is not the result of any act or omission which would constitute a default hereunder), or any failure or delay of any transportation, power, or communications system or any other or similar cause beyond that party's reasonable control. However, the inability to perform financial obligations hereunder shall not be construed as an event of Force Majeure.

14. Notice

14.1 Any notice required to be given to SLT shall be given in writing to the Deputy General Manager – Cloud Platforms, Sri Lanka Telecom PLC, Lotus Road, Colombo 1 or on Facsimile No: + 94 11 2387918 or to the e-mail address idcnotice@sltidc.lk

14.2 Any notice required to be given to the Customer shall be given to the person named under item 1.7 – Customer Contact in the Application for Virtual Server Hosting Service, which shall form an integral part hereof.

14.3 Any notice so given shall be deemed to have been duly given if sent as stated above (i) if delivered by hand, upon receipt thereof, (ii) if sent by registered post, three (03) working days after posting (iii) if sent by facsimile/e-mail transmission, upon electronic confirmation thereof.

15. Miscellaneous

15.1 Entire Agreement

This Agreement, Application and the Annexure hereof shall constitute the entire agreement between Customer and SLT with respect to the subject matter hereof and there are no representations, understandings or agreements that are not fully expressed in this Agreement.

15.2 Interpretation

In the event of a conflict between the terms of any Annexure and this Agreement, unless expressly stated otherwise in the Annexure, the provisions of this Agreement shall prevail.

15.3 Publicity

SLT may use the name and identify Customer as a SLT Customer, in advertising, publicity, or similar materials distributed or displayed to prospective Customers.

15.4 Relationship

SLT and its personnel, in the performance of this Agreement, are acting as independent contractors and not employees or agents of Customer. The provisions

hereof shall not be construed to interpret the Customer as the agent or employee of SLT.

15.5 Amendments

No amendment, change, waiver, or discharge hereof shall be valid unless it is in writing and signed by the authorized signatories of both parties.

15.6 Governing Law and Dispute Resolution

This Agreement shall be governed by the laws of the Democratic Socialist Republic of Sri Lanka. Any dispute arising between the parties if not amicably settled within 30 days, shall be referred to a Court of competent authority exercising jurisdiction in Sri Lanka.

15.7 Assignment

The rights and obligations of the Customer shall not be capable of assignment by the Customer without the prior written consent of SLT.

15.8 Waiver

The waiver or failure of either party to exercise any right provided for herein shall not be deemed a waiver of any further right hereunder.

Annex 1

Services

Annex 2

SLT Site Diagram (If available)

Annex 3

Fees and Payments

Annex 4

Customer support escalation matrix

Escalation Level	Operations Technical Support Management Level	Contact Details
1	24x7 IDC Help Desk	noc@sltidc.lk / dr@sltidc.lk
2	Engineer – iDC Operation Mr. Hansa Dilshan	Email: dilshanl@slt.com.lk
3	DGM – Cloud Platforms Mr. Prasad Rathnayake	Email: rathnayake@slt.com.lk
4	GM – Data Center and Cloud Mr. Ruchira Karunarathne	Email: ruchira21@slt.com.lk

Annex 5

Responsibilities of the Customer and SLT

Definitions

CSP	Cloud Service Provider
SLT	Sri Lanka Telecom
VM	Virtual Machine
VDC	Virtual Data Center
OS	Operating System
SSH	Secure Shell
RDP	Remote Desktop Protocol
VPN	Virtual Private Network
AV	Antivirus
RBAC	Role-Based Access Control
MFA	Multi-Factor Authentication
vCPU	Virtual Central Processing Unit
vRAM	Virtual Random Access Memory
PAM	Privileged Access Management
VA	Vulnerability Assessment
NLA	Network Level Authentication
SIEM	Security Information and Event Management
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
SLA	Service Level Agreement
DDoS	Distributed Denial of Service
OSS	Operations Support System
CRM	Customer Relationship Management
PII	Personally Identifiable Information
AM	Account Manager

	Customer Responsibilities	**Cloud Service Provider (SLT) Responsibilities**
1. Shared Roles and Responsibilities in a Cloud Computing Environment (CLD.6.3.1)	1.1 Virtual Machine (VM) & Virtual Data Center (VDC) Management • For individual VMs, the Cloud Service Provider (CSP) will provision the requested OS and configure access (SSH/RDP via VPN or	1.1 Security of Cloud Infrastructure • Maintain and secure the cloud platforms (e.g., VMware, Open Shift) to industry security standards. • Regularly patch hypervisors and

	internet). The CSP will provide initial credentials, which the customer must change immediately upon first login. Thereafter, the customer assumes full responsibility for VM security, maintenance, and management, and the CSP shall not be liable for any issues arising thereafter. • For Virtual Data Centers (VDCs), the Cloud Service Provider (CSP) shall provision the VDC with the agreed-upon resources and provide the tenant credentials to the customer. The customer is solely responsible for provisioning, managing, and upgrading virtual machines (VMs) within their VDC. The CSP will not be involved in VM creation, resource allocation, or modifications within the VDC at any stage. • The Customer is responsible for managing and securing all individual Virtual Machines (VMs) and VMs created within their assigned Virtual Data Centers (VDCs).	virtualization infrastructure. • Ensure physical security of data centers and high availability of infrastructure. 1.2 Service Provisioning and Access Control • Provision VMs with OS, vCPU, vRAM, and storage, and share initial credentials securely. • Enforce access control policies for cloud platform administrators. • Restrict publicly exposed management interfaces to authorized personnel only. 1.3 Security Monitoring & Logging • Monitor cloud platform activities for security events and unauthorized access. • Maintain logs of administrative actions and enforce compliance with access policies. 1.4 Incident Management & Service Assurance • Respond to faults and incidents reported via tickets or helpline. • Notify customers before planned maintenance or downtime. 1.5 Data Backup & Recovery • Provide a backup service as an optional offering (customers are responsible for enabling it).

	• The Customer must configure applications, databases, and security settings within their VMs. 1.2 Operating System and Software Security • The Customer must ensure that all operating systems and software installed on VMs are kept up to date with the latest security patches. • The Customer must implement and maintain antivirus (AV) and endpoint security solutions. 1.3 Data Protection and Backup • The Customer is responsible for encrypting sensitive data stored in their VMs and VDCs. • The Customer must manage and maintain backups unless they have purchased a backup service from the Cloud Service Provider (CSP). 1.4 User Access and Identity Management • The Customer must manage access credentials and enforce role-based access control (RBAC) for users accessing their VMs and applications. • Multi-Factor Authentication (MFA) is strongly	• CSP is not responsible for customer data loss if the backup service is not used. 1.6 Service Termination & Data Retention • Disable VMs/VDCs upon service termination and retain them for one month before deletion. • Allow customers to retrieve their data during the retention period.

	recommended for administrative and privileged accounts.	
2. Secure Removal of Cloud Customer Assets (CLD.8.1.5)	2.1 Data Backup and Retention Before Termination • The Customer must take backups of their data before requesting service termination. • If the Customer has purchased the CSP's backup service, they must restore their data before permanent deletion. 2.2 Secure Data Deletion from VMs/VDCs • Before termination, the Customer must securely erase or encrypt sensitive data to prevent unauthorized access. • The Customer should use secure deletion tools or encryption methods to protect residual data. 2.3 Access Revocation and Service Decommissioning • The Customer must decommission user access to their applications running in the cloud before service termination. • Third-party integrations must be disabled before VM/VDC deletion. 2.4 Compliance with Data Protection Regulations • The Customer is responsible for ensuring compliance with internal policies,	2.1 Secure Data Deletion • After the one-month grace period, permanently delete customer VMs/VDCs. • Ensure secure deletion methods 2.2 Prevent Unauthorized Access to Decommissioned Resources • Restrict access to deactivated VMs during the retention period. • Remove any CSP-managed credentials associated with terminated resources. 2.3 Audit and Compliance Logging • Maintain logs of asset decommissioning, including timestamps and deletion confirmations. • Keep audit trails for compliance and future reference.

	industry standards, and regulatory requirements when decommissioning cloud resources.	
3. Segregation in Virtual Computing Environments (CLD.9.5.1)	3.1 Secure Configuration of Virtual Machines and VDCs • The Customer must configure their VMs and applications to prevent unauthorized access. • The Customer should implement network segmentation within their VDCs (e.g., separate production and development environments). 3.2 Data Protection and Encryption • The Customer must encrypt sensitive data within VMs to protect against unauthorized access. • File system and database-level encryption are strongly recommended. 3.3 Network Security Measures • The Customer must configure firewalls within VMs and VDCs to restrict access to authorized IPs only. • Proper segmentation between internal services must be maintained to prevent lateral movement in case of a breach.	3. Segregation in Virtual Computing Environments (CLD.9.5.1) 3.1 Isolation of Customer Environments • Ensure that customer VMs are logically and network-wise isolated from other tenants. • Use VLANs, SDN, and firewall rules to enforce multi-tenancy security. 3.2 Security Monitoring & Compliance • Monitor for misconfigurations that could lead to data leakage or unauthorized access. • Conduct regular security assessments to ensure compliance with segregation policies. 3.3 Role-Based Access for CSP Operations • Implement Privileged Access Management (PAM) to secure administrative access. • Restrict CSP administrator access to customer environments only upon approval.

4. Virtual Machine Hardening (CLD.9.5.2)	4.1 OS Hardening & Security Configurations • The Customer must apply security baselines (e.g., CIS Benchmarks, vendor security guides) to harden OS configurations. • The Customer must disable unnecessary services, ports, and accounts on VMs. 4.2 Patch Management & Vulnerability Remediation • The Customer must regularly update their operating systems and applications to address security vulnerabilities. • Vulnerability assessments (VA) should be conducted to identify and mitigate risks. 4.3 Access Control & Identity Management • The Customer must enforce least privilege access and use role-based access control (RBAC) for VM administrators. • Multi-Factor Authentication (MFA) is strongly recommended. 4.4 Network Security and Monitoring • The Customer must implement host-based firewalls and restrict remote access	4.1 Secure VM Deployment • Provide pre-configured hardened OS images with essential security patches. • Regularly update VM templates to address new vulnerabilities. 4.2 Network & Access Security • Maintain secure hypervisor configurations to protect against exploits. • Use firewall rules and VLANs to prevent unauthorized cross-tenant access. 4.3 Security Monitoring & Threat Detection • Monitor cloud infrastructure for security incidents and suspicious activities. • Provide logs or alerts to customers if malicious activity is detected. 4.4 Secure VM Decommissioning • Retain disabled VMs for one month, then securely delete them. • Ensure data sanitization before reusing storage resources.

	(SSH/RDP) to trusted IPs only. • Security monitoring and logging must be enabled on all VMs.	
5. Administrator's Operational Security (CLD.12.1.5)	5.1 Secure Administrative Access • The Customer must enforce role-based access control (RBAC) for VM and application administrators. • The least privilege principle must be followed to minimize exposure to critical systems. 5.2 Credential and Password Management • The Customer must rotate administrator credentials regularly and enforce strong password policies. • Shared admin accounts must be avoided to maintain accountability. 5.3 Monitoring and Logging of Admin Activities • The Customer must enable logging and monitoring of administrative actions on VMs and applications. • Regular log reviews should be conducted to detect suspicious activity. 5.4 Secure Remote Administration • The Customer must restrict remote admin	5.1 Secure Administrative Access • Implement Privileged Access Management (PAM) for secure admin authentication. • Restrict CSP admin access to customer environments only for support purposes. • Enforce Multi-Factor Authentication (MFA) for CSP administrators. 5.2 Logging & Monitoring of CSP Admin Actions • Log all CSP administrator actions related to customer environments. • Ensure logs are tamper-proof and retained for compliance. 5.3 Infrastructure Patching & Hardening • Regularly patch virtualization platforms (VMware, OpenShift) to fix vulnerabilities. • Apply industry best practices to secure cloud infrastructure components. 5.4 Secure Communication of Credentials • Move towards secure credential management (e.g., password vaults, temporary credentials).

	access to trusted IP addresses. • Secure protocols such as SSH key-based authentication and RDP Network Level Authentication (NLA) should be used.	• Improve current credential-sharing methods (e.g., avoid email-based sharing).
6. Monitoring of Cloud Services (CLD.12.4.5)	6.1 Performance Monitoring of VMs and Applications • The Customer must monitor resource usage, system health, and uptime to detect performance issues. • Logs, alerts, and dashboards should be utilized for proactive monitoring. 6.2 Security Event Monitoring • The Customer must enable logging of security-related events, including failed logins and privilege escalation attempts. • Security Information and Event Management (SIEM) systems should be used for centralized log analysis. 6.3 Patching and Vulnerability Management • The Customer must apply security patches regularly to reduce security risks. • Vulnerability scanning tools should be used to detect and address system weaknesses. 6.4 Backup and Data Integrity Monitoring	6.1 Infrastructure & Platform Monitoring • Continuously monitor cloud infrastructure health, performance, and resource utilization. • Detect and respond to performance bottlenecks and security incidents. 6.2 Network & Security Monitoring • Implement intrusion detection and prevention systems (IDS/IPS). • Monitor network traffic for unusual activity or attacks. 6.3 Security Logging & Incident Response • Log all CSP administrative actions on the platform. • Investigate and respond to security incidents affecting multiple customers. 6.4 Service Level Agreement (SLA) Compliance • Ensure uptime and availability as per SLAs (if applicable). • Notify customers about planned and unplanned service outages.

	• The Customer must verify backup processes and ensure that backup data remains intact. • Regular backup integrity tests should be performed.	
7. Alignment of security management for virtual and physical networks (CLD.13.1.4)	7.1 VM and Application Network Security • The Customer must configure firewall rules, security groups, and network segmentation to limit access. • Host-based security controls (e.g., iptables, Windows Firewall) should be used where applicable. 7.2 Network Access Controls • The Customer must restrict SSH/RDP access based on least privilege principles. • Network configurations should be reviewed regularly for security compliance. 7.3 Patch Management for Network Components in VMs • The Customer must update OS and network-related components (e.g., OpenSSH, VPN software) regularly. • Vulnerability scans should be conducted to detect outdated network configurations. 7.4 Compliance with CSP's Network Security Policies • The Customer must follow the CSP's	7.1 Data Center & Network Security • Secure physical network infrastructure (e.g., firewalls, routers, switches). • Implement DDoS protection and network intrusion detection. • Ensure customer traffic is isolated to prevent cross-tenant attacks. 7.2 Segmentation of Virtual Networks (VDCs & Containers) • Enforce strong access controls for virtual networks (VDC, Kubernetes, and containers). • Restrict public-facing access to admin consoles (e.g., OpenShift, vCloud Director). 7.3 Security Monitoring & Incident Response • Monitor network traffic at the hypervisor level for threats. • Investigate and respond to network-related security incidents. 7.4 Network Security Best Practices for Customers • Provide security guidelines for VM networking, firewall

	security guidelines for segmentation, access control, and secure network practices. • Compliance with security best practices is required when configuring network services inside the cloud. 7.5 Business Continuity & Disaster Recovery • The Customer must establish redundancy, and failover plans for applications running on VMs/VDCs. • Disaster recovery mechanisms should be tested regularly.	configurations, and segmentation. • Offer recommendations for VPN usage, encryption, and best practices. 7.5 Service Availability & Load Balancing • Ensure network redundancy to minimize service disruptions. • Improve failover processes to enhance cloud service resilience.
8. PII Compliance	• Provide accurate administrator contact information (email/phone). • Do not share unnecessary personal data with CSP • Reset all default credentials immediately after access. Restrict VM access to authorized personnel. • Notify CSP of administrator changes promptly. • Monitor VMs for suspicious activity. Report VM security incidents to CSP within 72 hours. • Remove all sensitive data from VMs before termination.	• Communicate how customer contact details are used (account setup/support only). Never uses customer data for advertising. • Only collects necessary details (admin name/email). Never requests sensitive IDs (passports, etc.). • Encrypts customer contact details (OSS). Provides temporary VM credentials (expire after first use). • Maintains up-to-date contacts when notified (AM updates vis CRM) • Notifies customer within 72 hours of contact data breaches. Addresses CSP-side vulnerabilities.

	• Approve/reject subcontractors per contract terms. • Specify permitted/disallowed data locations. • Full responsibility for OS/application maintenance, patching, performance monitoring and troubleshooting. Must manage all VM credentials without CSP involvement. • It is the responsibility of the customer to execute remediation actions (ex. Restart VMs, Scale resources, Apply patches)	• Notifies customer within 72 hours of contact data breaches. Addresses CSP-side vulnerabilities. • Discloses all subcontractors handling customer data. Requires subcontractor compliance. • Discloses data storage jurisdictions. • Under no circumstances will CSP personnel log into customer VMs • Only involved in providing non-intrusive recommendations (ex. VM is at 95% memory utilization) in cases where customer lodge a complaint.

Annex 6

VMware - Service Level Agreement

1. Introduction

This Service Level Agreement for SLT VMware Cloud Services (**this "SLA"**) is a part of your SLT Virtual Hosting with VMware Cloud customer agreement (the "Agreement"). And here affiliates (**"SLT," "we," "us,"** or **"our"**) and you or the entity you represent (**"you"**).

We will not modify the terms of your SLA during the initial term of your subscription; however, if you renew your subscription, the version of this SLA that is current at the time of renewal will apply throughout your renewal term. We will provide at least 60 days' notice for adverse material changes to this SLA.

2. General Terms

Definitions

2.1 **Month** will be defined as a period from the first to the last day of the month, unless otherwise specified.

2.2 **Year** shall be defined as the period from the first day to the last day of the calendar year, unless otherwise specified.

2.3 **Service** means the use of VMware compute resources, applications, software, connectivity, features related to connectivity such as routing, firewalls, load balancing or content provided or any other services made available by us or our affiliates, including support services.

2.4 **Service Outage** is defined as a condition under which, it is impossible to use the 'service' provided by VMware Cloud platform.

Service Outage is measured from the time the trouble ticket is opened for the Affected Service to the time the Affected Service is again able to use without disruption Service Outage is defined for each service constituting the **VMware Cloud Services.**

2.5 **Availability** Percentage of uptime for a service in a given observation period.

$$\textbf{Availability} = \frac{\text{(Total number of contracted hours - total number of outage hours)} \times 100\%}{\text{Total number of contracted hours}}$$

Availability is defined for each service constituting the **VMware Cloud Services** on monthly basis.

2.7 **Downtime** is defined for each Service in the Services Specific Terms below. Downtime does not include Scheduled Downtime. Downtime does not include unavailability of a Service due to limitations described below and in the Services Specific Terms.

2.8 **Incident** means (i) any single event, or (ii) any set of events, that result in Downtime.

2.9 **Management Portal** means the web interface, provided by SLT, through which Virtual Data Center customers may manage the Service.

2.10 **Scheduled Downtime** means periods of Downtime related to network, hardware, or Service maintenance or upgrades. We will publish notice or notify you at least five (5) days prior to the commencement of such Downtime.

2.11 **Service Level** means the performance metric(s) set forth in this SLA that SLT agrees to meet in the delivery of the Services.

3. Description of Services

This service level agreement shall be subject to the following conditions.

3.1 These service levels shall be applicable for each service constituting the **VMware Cloud Services.**

3.2 The service mentioned under (2.3) above are,
[Description of the services] **Service"** means the use of VMware compute resources, applications, software, connectivity, features related to connectivity such as routing, firewalls, load balancing or content provided or any other services made available by us or our affiliates, including support services.

3.3 Faults that are beyond the control of SLT, such as any issues arising from the use of third party provided content or applications which obstruct the effective functioning of the service are not covered under this service level agreement.

4. *Service Levels*

4.1 Availability.

Availability of the **VMware Cloud Services** described under section 2.5 of this agreement shall be as follows on a monthly basis.

Monthly Availability of VMware Cloud Services equal to or greater than 99.9%

5. Fault Reporting

5.1 Fault reporting would be from one of the authorized Contact Persons of CUSTOMER.

An acknowledgment of the call with a reference number will be given to the CUSTOMER Contact Person reporting the call, for CUSTOMER's future references.

5.2 Fault reporting will be done by CUSTOMER's Contact Person at:

IDC Help Desk
Telephone number: 011-2399121 (24x7)
Email: noc@sltidc.lk

5.3 CUSTOMER shall log all calls at SLT IDC Help Desk with following details:

- CCT ID for the services
- Brief description of problem
- Reporting Contact Person's Name from
- Any other useful information that may be useful in resolving the fault

5.4 Hours of Services:
The Calls will be logged in and attended on 24X7 basis.

5.5 CUSTOMER shall follow a logical procedure to localize the problem before fault reporting and escalation.

5.6 CUSTOMER staff members listed under customer contact in Application form shall be the technical points of contact from the CUSTOMER's side and will assist/coordinate with SLT technical team in the fault restoration procedure.

6. Restoration of Faults

6.1 Maintenance Window: 24 hours, seven days a week

7. Limitations

This SLA and any applicable Service Levels do not apply to any performance or availability issues:

1. Due to factors outside our reasonable control (for example, natural disaster, war, acts of terrorism, riots, government action, or a network or device failure external to our data centers, including at your site or between your site and our data center);
2. That result from the use of application or software provided by a third party.
3. Caused by your use of a Service after we advised you to modify your use of the Service, if you did not modify your use as advised;
4. During or with respect to preview, pre-release, beta or trial versions of a Service, feature or software (as determined by us);
5. That result from your unauthorized action or lack of action when required, or from your employees, agents, contractors, or vendors, or anyone gaining access to our network by means of your passwords or equipment, or otherwise resulting from your failure to follow appropriate security practices;
6. That result from your failure to adhere to any required configurations, use supported platforms, follow any policies for acceptable use, or your use of the Service in a manner inconsistent with the features and functionality of the Service (for example, attempts to perform operations that are not supported) or inconsistent with our published guidance;
7. That result from faulty input, instructions, or arguments (for example, requests to access files that do not exist);
8. That result from your attempts to perform operations that exceed prescribed quotas or that resulted from our throttling of suspected abusive behavior;
9. Due to your use of Service features that are outside of associated Support Windows; or
10. For licenses reserved, but not paid for, at the time of the Incident.