Annex A
(normative)

Cloud service provider disclosure

The form is to be completed for each cloud service provided. For questions not applicable or not disclosed, indicate accordingly in the remarks.

Cloud Service Provider Contact Information
Company name: Wizlearn Technologies Pte Ltd
Primary address: 10 Science Park Road #03-13
The Alpha, Singapore Science Park II
Singapore (117684)
Web address: www.wizlearn.com
Contact name: NG MIEN TA
Contact number: +65 9180 6488
MTCS Certificate Number MTCS-2016-0004
Company Chop _____ Company Representative Signature: _____
Certification Body Contact Information
Company name: TUV-SUD-PSB
Web address: www.tuv-sud-psb.sg
Contact name: Nur Kamal Bin Kamari
Contact email: kamal.kamari@tuv-sud-psb.sg
Company Chop _____ Lead Auditor Signature: _____
Cloud Service Provider Background
Overview of service offering:
Provision of e-learning solution using SAAS model.
Service model:
☐ Virtual machine instances owned by the user
☐ Network facilities

(Company Chop stamp: WIZLEARN TECHNOLOGIES PTE. LTD.)

(Company Chop stamp: TÜV SÜD PSB Pte Ltd, 1 Science Park Drive, Singapore 118221, Tel : +65 6778 7777 Fax : +65 6779 7088, Co. Reg. No : 199002667R)

☑ Compliance with applicable standards

Deployment model:

☑ Private cloud

☐ Community cloud

☐ Hybrid cloud

☐ Public cloud

Tier:

☐ Level 1

☑ Level 2

☐ Level 3

No.	Criteria	Description	Remarks
		Legal and Compliance	
1.	Right to audit	The user has the right to audit: ☐ Virtual machine instances owned by the user ☐ Network facilities ☑ Compliance with applicable standards ☐ Technical controls ☑ Policies and governance ☐ Data centre facilities ☐ Others _____ ☐ None Regulators recognised by Singapore law have the right to audit: ☐ Virtual machine instances owned by the user ☐ Network facilities ☑ Compliance with applicable standards ☐ Technical controls ☑ Policies and governance ☐ Data centre facilities ☐ Others _____	

		☐ None Audit / assessment reports that can be made available on request: ☑ Penetration test ☐ Threat and vulnerability risk assessment ☐ Vulnerability scan ☐ Audit reports (e.g. Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organisation)	
2.	Compliance	The following guidelines / standards / regulations are adhered to: ☑ Singapore Personal Data Protection Act ☑ ISO / IEC 27001 ☐ ISO 9000 ☐ ISO / IEC 20000 ☐ CSA Open Certification Framework ☐ PCI-DSS ☐ Others _____	
Data Control			
3.	Data ownership	All data on the cloud service is owned by the cloud user except for: Learning Management System source code _____ The cloud User retains the ownership on the derived data or attributes of cloud usage except for the following: ☐ Advertising or marketing ☐ Statistics analysis on usage ☐ Others_____	
4.	Data retention	Data deleted by the user is retained as follows: ☐ Minimum data retention period is: _____ ☐ Maximum data retention period is: _____ ☑ Deleted immediately Log data is retained for a period of: ☐ Minimum data retention period as follows: _____ ☑ Maximum data retention period is: 6 months	

		☐ Not retained User data is retained for a period of: ☐ Minimum data retention period is: _____ ☐ Maximum data retention period is: _____ ☑ Not retained The following types of data are available for download by the cloud user: ☐ Log data ☐ Other _____	
5.	Data sovereignty	The primary data locations are: ☑ Singapore ☐ Asia Pacific _____ ☐ Europe_____ ☐ United States ☐ Other _____ The backup data locations are: ☑ Singapore ☐ Asia Pacific_____ ☐ Europe_____ ☐ United States ☐ Other _____ No. of countries in which data centres are operated: _____ The user's data stored in the cloud environment will never leave the locations specified in item 5: ☑ Yes ☑ Yes, except as required by law ☑ Yes, except as noted: Upon customer request _____ ☐ No	

		User's consent is required prior to transferring data to a location not specified in item 5 or a third party: ☑ Yes ☑ Yes, except as required by law ☑ Yes, except as noted: Upon customer request ☐ No *Note: Cloud users are responsible for determining the impact of data protection and data sovereignty laws on the locations where data is stored. In addition, users should understand the risks associated with relevant laws that may allow for law enforcement or other government access to data in-transit or storage with Cloud Service Providers.*	
6.	Non-disclosure	☑ Non-disclosure agreement template can be provided by Cloud Service Provider ☑ Cloud Service Provider may use customer's NDA (pending legal review)	
Provider Performance			
7.	Availability	The committed network uptime is: ☑ _____99_____ % ☐ Varies according to price plan The committed system uptime is: ☑ _____99_____ % ☐ Varies according to price plan The cloud environment has the following single points of failure: ☐ _____ ☑ none	
8.	BCP / DR	☑ Disaster recovery protection ☑ Backup and restore service ☐ User selectable backup plans ☐ Escrow arrangements ☐ No BCP / DR is available ☑ RPO On contract agreement ☑ RTO On contract agreement	

		☐ Others, please specify: _____ _____	
9.	Liability	The following terms are available for the users on failure of the provider to meet the service commitment: ☐ Network failure Liability: _____ ☐ Infrastructure failure Liability: _____ ☐ Virtual machine instance failure Liability:_____ ☐ Migrations Liability:_____ ☐ Unscheduled downtime Liability:_____ ☐ Database failure Liability:_____ ☐ Monitoring failure Liability:_____	
Service Support			
10.	Change management	The Cloud Service Provider has established the following for changes, migrations, downtime, and other potential interruptions to cloud services: ☑ Communication plan and procedures for proactive notification ☑ Assistance in migration to new services when legacy solutions are discontinued ☑ Ability to remain on old versions for a defined time period ☐ Ability to choose timing of impact	
11.	Self-service provisioning and management portal	Provide self-service provisioning and management portal for users to manage cloud services: ☐ Yes ☑ No If yes, describe the functions of the self-service provisioning and	

		management portal provided: ☐ Allow role-based access control (RBAC) ☐ Manage resource pools (e.g. VMs, storage, and network) and service templates ☐ Track and manage the lifecycle of each service ☐ Track consumption of services ☐ Others: _____	
12.	Incident and problem management	Delivery mode of support: ☑ Access via email ☐ Access via portal ☑ Access via phone support ☑ Direct access to support engineers Availability of support: ☑ 24 x 7 ☑ During office hours support, please specify the hours of operations: _730am to 900pm_____ ☐ After office hours support, please specify the hours of operations: _____ Service response time: _4hrs (based on sev1 classification)____ The following are available to users upon request: ☐ Permanent access to audit records of customer instances ☑ Incident management assistance Incident response time: _2hrs (based on sev1 classification)___ Mean time to repair on detection of faults: _____	
13.	Billing	The following billing modes are available (please elaborate granularity of charges and measurement): ☐ Pay per usage _____ (up to per min/hour/day/month for compute/storage for IaaS/PaaS, and per user per hour/day/month/year for SaaS) ☐ Fixed pricing_____(up to yearly/monthly/daily) ☑ Other pricing model_____	

		☐ Not disclosed	
		☐ Available billing history: _____Months	
14.	Data portability	Importable VM formats: _____ Downloadable formats: office format, zip, 7z _____ Supported operating systems: _____ Language versions of supported operating systems: _____ Supported database formats: bak _____ API: ☐ Common _____ ☐ Customised _____ Upon service termination, data is available through: ☑ Physical media ☐ Standard methods as described above ☐ Other methods _____ _____	
15.	Access	Type of access to the service is through: ☑ Public access ☑ Private access (e.g. VPN, dedicated link) ☐ IPv6 access is supported ☐ Other access methods _____ _____ _____ Public access speed (shared bandwidth) in Mbps: _____	
16.	User management	☐ Identity management ☑ Role based access control ☐ Federated access model ☐ Integration with Identity management solutions ☐ Others_____	

17.	Lifecycle	The cloud user may select the following for service upgrades and changes: ☐ Automatic provisioning ☑ User customisable provisioning	
Security Configurations			
18.	Security configuration enforcement checks	Security configuration enforcement checks are performed: ☑ Manually ☑ Using automated tools How often are enforcement checks being performed to ensure all security configurations are applied? As when new update/fixes to the application code. External audits done annually.	
19.	Multi-tenancy	☑ Distinct physical hosts ☐ Distinct physical network infrastructure ☑ Virtual instance grouping ☐ User definable security domains ☐ User customisable firewall ☐ User definable access policies	
Service Elasticity			
20.	Capacity elasticity	The following capacity elasticity options are available: ☐ Programmatic interface to scale up or down ☐ Mean time to start and end new virtual instances _____ ☑ Alerts to be sent for unusual high usage ☐ Minimum performance during peak periods_____ ☐ Minimum duration to scale up computing resources _____ ☐ Minimum additional capacity guaranteed per account _____ (number of cores and GB memory)	
21.	Network resiliency and elasticity	The following network resiliency and elasticity options are available: ☑ Redundant Internet connectivity links ☑ Redundant Internal connectivity ☑ Selectable bandwidth up to _____Mbps ☐ Maximum usable IPs _____	

		☑ Load balancing ports_____ ☐ Load balancing protocols_____ ☑ Anti-DDOS protection systems or services ☑ Defence-in-depth mechanisms, please specify: _____ WAF, Firewall, IDS, IPS _____ _____ ☐ Network traffic isolation, please specify: _____ _____ ☑ Shared or dedicated bandwidth, please specify: _____ Based on customer requirement _____ ☐ QoS traffic control services ☑ Alerts to be sent for unusual high usage ☐ Minimum performance during peak periods_____ ☐ Minimum period to scale up network throughput _____	
22.	Storage redundancy and elasticity	The following storage redundancy and elasticity options are available: ☐ Redundant storage connectivity links within each data centre ☑ Redundant storage connectivity links between data centres belonging to the same cloud ☐ Storage traffic isolation, please specify: _____ _____ ☐ Shared or dedicated storage network bandwidth, please specify: _____ ☐ Quality of service storage traffic control services ☐ Maximum storage capacity for entire cloud, please specify: _____ ☑ Maximum storage capacity for single user, please specify: _____ ☐ Maximum expandable storage, please specify: _____ ☑ Alerts to be sent for unusual high usage	

		☐ Minimum storage I / O performance during peak periods	
		☐ Minimum period to scale up storage I / O throughput	