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: Starhub

Primary address: 67, Ubi Ave 1,#05-01

　　　　　　　　Starhub Green, (S)408942

Web address: www.starhub.com

Contact name: Marcus Tay

Contact number: 93661412

Acknowledgement:

Sunny Tan Chung Yung

Assistant Vice President (EBG Solutions)

Certification Body Contact Information

Company name: TUV SUD PSB Pte Ltd

Web address: www.tuv-sud-psb.sg

Contact name: Chris Ng

Contact email: khee-soon.ng@tuv-sud-psb.sg

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

Shawn Hea Chuay
Operations Manager
4/11/14

Cloud Service Provider Background

Overview of service offering:

Argonar is an agile and flexible Infrastructure-as-a-Service (IaaS) platform that allows customer to manage compute resources with ease. Customers are better-equipped to adapt to the changing demands of their business without the hefty costs of infrastructure and the burden of managing it. Customers can enjoy the freedom of seeing their business soar to greater heights.

Service model:

☑ Virtual machine instances owned by the user

☑ Network facilities

☑ Compliance with applicable standards

Deployment model:

☐ Private cloud

☐ Community cloud

☑ Hybrid cloud

Tier:	☑ Public cloud
	☑ Level 1
	☐ Level 2
	☐ Level 3

No.	Criteria	Description	Remarks
	Legal and Compliance		
1.	Right to audit	The user has the right to audit:	StarHub can share the ISO 27001 audit. The certification, scope and statement of applicability can be made available upon request
		☑ 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	Penetration test and risk assessment is performed regularly
		☑ Threat and vulnerability risk assessment	
		☑ Vulnerability scan	A summary can be

		☐ Audit reports (e.g. Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organisation)	made upon request .
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 _____	Certification no. IS27-2013-0038
Data Control			
3.	Data ownership	All data on the cloud service is owned by the cloud user except for: <u>IP rights of the Cloud platform.</u> 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: _____ ☐ Not retained User data is retained for a period of: ☐ Minimum data retention period is: _____ ☐ Maximum data retention period is: _____	VM image will be kept on system for at least 1 month after deletion. Customer data volume is with immediate deleted User Data is stored in their user disk which is managed by their own administrator. Once they delete the acquired disk, all data is wiped

		☑ Not retained The following types of data are available for download by the cloud user: ☐ Log data ☐ Other _____	Log data download not allowed. However, can be provided upon request.
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: __1_____ 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: _____ ☐ 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	No backup site yet.

		☐ Yes, except as noted: _____ ☐ 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: ☑ <u>99.95</u> % ☐ Varies according to price plan The committed system uptime is: ☑ <u>99.95</u> % ☐ Varies according to price plan The cloud environment has the following single points of failure: ☐ _____ ☑ none	No single point of failure.
8.	BCP / DR	☐ Disaster recovery protection ☑ Backup and restore service ☐ User selectable backup plans ☐ Escrow arrangements ☐ No BCP / DR is available ☑ RPO <u>24 hrs</u> ☑ RTO <u>9 hrs</u> ☐ Others, please specify: _____ _____	
9.	Liability	The following terms are available for the users on failure of the provider to meet the service commitment:	Subject to SLA

			agreement terms and conditions
		☑ 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: 8 x 5 _____ ☐ After office hours support, please specify the hours of operations: _____ Service response time: Critcal cases <30 mins, major cases < 24 hrs The following are available to users upon request: ☑ Permanent access to audit records of customer instances ☑ Incident management assistance Incident response time: Critcal cases <30 mins, major cases < 24 hrs Mean time to repair on detection of faults: Critical case is 6 hrs service restore time. Major is 48 hours.	Direct access to support engineers when case is escalated and cannot be resolved at Tier 1 and 2 support. 24 x 7 Customer Services support Customer hasfull access rights to their audit records on their VMs For Cloud infra related incidents only.
13.	Billing	The following billing modes are available (please elaborate granularity of charges and measurement): ☑ Pay per usage compute units per hour (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 monthly (up to yearly/monthly/daily) ☐ Other pricing model_____ ☐ Not disclosed	Cloud Metering Gateway can capture up to per min usage of cloud resources.

		☐ Available billing history: _____Months	
14.	Data portability	Importable VM formats: ISO Downloadable formats: ISO Supported operating systems: <u>Windows, RHEL, CentOS, Ubuntu.</u> Language versions of supported operating systems: <u>Any languages support by the OS.</u> Supported database formats: <u>Any database that can be installed on supported Operating system above.</u> 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: <u>1 Gbps</u>	IPv6 ready in Q1 2014.
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? elog server is on-going 24 x 7 monitoring.	Automated log is using eLog to proactively alert support on security events.
19.	Multi-tenancy	☐ Distinct physical hosts ☐ Distinct physical network infrastructure ☑ Virtual instance grouping ☑ User definable security domains ☑ User customisable firewall ☑ User definable access policies	All physical server and network hardware are shared resources. Hybrid options are available
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 _3 – 5 mins_ ☑ 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 _50_ Mbps per VM ☑ Maximum usable IPs As per user's requirements, it is scalable	

		☐ Load balancing ports ☐ Load balancing protocols_____ ☑ Anti-DDOS protection systems or services ☑ Defence-in-depth mechanisms, please specify: <u>Firewall has in-built IDS / IPS capabilities. Security groups in the form of 3-tier zones - web, apps and database</u> ☑ Network traffic isolation, please specify: <u>split into 3 VLANs (Service, Management & Storage)</u> ☑ Shared or dedicated bandwidth, please specify: <u>Shared</u> _____ ☐ QoS traffic control services ☑ Alerts to be sent for unusual high usage ☑ Minimum performance during peak periods <u>10 Mbps</u> ☐ 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: <u>it's dedicated storage traffic (storage zone) layer 2</u> ☑ Shared or dedicated storage network bandwidth, please specify: <u>Dedicated. Multi path with total 8Gbps bandwidth.</u> ☐ Quality of service storage traffic control services ☑ Maximum storage capacity for entire cloud, please specify: <u>No maximum. Additional storage will be added when current utilisation hit >70%.</u> ☑ Maximum storage capacity for single user, please specify: <u>Based on user subscription to Storage volumes.</u>	

		☑ Maximum expandable storage, please specify: 4608 TB ☑ 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	