Cloud Service Provider Disclosure (SS 584:2020 MTCS)

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

Date of disclosure: _____

Applicable cloud service(s): _____

Cloud Service Provider Contact Information

Company name: _____

Primary address: _____

_____

_____

Web address: _____

Contact name: _____

Contact number: _____ Contact email: _____

MTCS certificate number: _____

Company stamp: _____ Company representative signature: _____

Certification Body Contact Information

Company name: _____

Web address: _____

Contact name: _____

Contact number: _____ Contact email: _____

Company stamp: _____ Lead auditor signature: _____

Cloud Service Provider Background

Overview of service offering:

_____

_____

_____

Service model:

☐ Virtual machine instances owned by the cloud service customer

☐ Network facilities

☐ 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 cloud service customer has the right to audit: ☐ Virtual machine instances owned by the cloud service customer ☐ 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 cloud service customer ☐ 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 service customer except for: _____ The cloud service customer 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 cloud service customer 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 Cloud service customer 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 service customer: ☐ Log data ☐ Others _____	
5.	Data sovereignty	The primary data locations are: ☐ Singapore ☐ Asia Pacific _____ ☐ Europe _____ ☐ United States ☐ Others _____ The backup data locations are: ☐ Singapore ☐ Asia Pacific _____ ☐ Europe _____ ☐ United States ☐ Others _____ No. of countries in which data centres are operated: _____ The cloud service customer'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 Cloud service customer'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: _____ ☐ No *Note: Cloud service customers are responsible for determining the impact of data protection and data sovereignty laws on the locations where data is stored. In addition, cloud service customers 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: ☐ _____% ☐ Varies according to price plan The committed system uptime is: ☐ _____% ☐ Varies according to price plan The cloud environment has the following single points of failure: ☐ _____ ☐ none	
8.	3rd party dependency	Highlight areas of critical dependency for service delivery: _____ _____	
9.	BCP / DR	☐ Disaster recovery protection	

		☐ Backup and restore service ☐ Cloud service customer selectable backup plans ☐ Escrow arrangements ☐ No BCP / DR is available ☐ RPO _____ ☐ RTO _____ ☐ Others, please specify: _____ _____	
10.	Liability	The following terms are available for the cloud service customers 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: _____	
11.	Shared responsibility	☐ Communication of shared roles & responsibilities for which CSC needs to implement and manage for use of this cloud service URL (or attach file): _____	
Service Support			
12.	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	
13.	Self-service provisioning and management portal	Provide self-service provisioning and management portal for cloud service customers 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 ☐ Health monitoring ☐ Others: _____ _____	
14.	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: _____ ☐ After office hours support, please specify the hours of operations: _____ Service response time: _____	

		Notification time of cloud service outage incident: _____ Communication channel used for notification of cloud service outage incident: _____ The following are available to cloud service customers upon request: ☐ Permanent access to audit records of customer instances ☐ Incident management assistance Incident response time: _____ Mean time to repair on detection of faults: _____	
15.	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 cloud service customer per hour/day/month/year for SaaS) ☐ Fixed pricing _____ (up to yearly/monthly/daily) ☐ Other pricing model _____ ☐ Not disclosed ☐ Available billing history: _____ months	
16.	Data portability	Importable VM formats: _____ Downloadable formats: JSON/XML/other open formats (to specify) _____ Supported operating systems: _____ Language versions of supported operating systems: _____ Supported database formats: _____ Policy/guide available: _____ API: ☐ Common _____ ☐ Customised _____ Upon service termination or prolonged outage, data is available through:	

		☐ Physical media ☐ Standard methods as described above ☐ Other methods _____ _____	
17.	Interoperability	Use of industry standards and availability of APIs to support interoperability: ☐ Transport supported (e.g. REST based HTTPS/MQTT) _____ ☐ Format supported (e.g. JSON/XML) _____ ☐ APIs supported _____ ☐ Other methods _____ _____ Guide available _____	
18.	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: _____	
19.	User management	☐ Identity management ☐ Role based access control ☐ Federated access model ☐ Integration with Identity management solutions ☐ Others _____	
20.	Lifecycle	The cloud service customer may select the following for service upgrades and changes: ☐ Automatic provisioning ☐ Cloud service customer customisable provisioning	

Security Configurations			
21.	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? _____	
22.	Multi-tenancy	☐ Distinct physical hosts ☐ Distinct physical network infrastructure ☐ Virtual instance grouping ☐ Cloud service customer definable security domains ☐ Cloud service customer customisable firewall ☐ Cloud service customer definable access policies	
23.	Hybrid cloud provision	Ability to monitor, track, apply and enforce CSC's security & privacy policies on its cloud workloads: ☐ Data protection and encryption key mgmt. enforcement geolocation-based/resource pools and secure migration of cloud workloads ☐ Key mgmt. and keystore controlled by CSC ☐ Persistent data flow segmentation before and after geolocation-based/resource pools secure migration ☐ Compliance enforcement for regulated workloads between on-premises private and hybrid/public cloud ☐ Others _____	
Service Elasticity			
24.	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)	
25.	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: _____ _____ _____ ☐ Network traffic isolation, please specify: _____ _____ ☐ Shared or dedicated bandwidth, please specify: _____ _____ ☐ QoS traffic control services ☐ Alerts to be sent for unusual high usage ☐ Minimum performance during peak periods _____ ☐ Minimum period to scale up network throughput _____	
26.	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 cloud service customer, 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 _____	