

Cloud service provider disclosure (SS 584:2026 MTCS)

This form shall 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:

- ☐ IaaS
- ☐ PaaS
- ☐ SaaS

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	<p>The cloud service customer (CSC) has the right to audit:</p> <ul style="list-style-type: none">☐ VM instances owned by the CSC☐ Network facilities☐ Compliance with applicable standards☐ Technical controls☐ Policies and governance☐ Data centre facilities☐ Others: _____☐ None	

		<p>Regulators recognised by the local jurisdiction have the right to audit:</p> <p>☐ VM instances owned by the CSC</p> <p>☐ Network facilities</p> <p>☐ Compliance with applicable standards</p> <p>☐ Technical controls</p> <p>☐ Policies and governance</p> <p>☐ Data centre facilities</p> <p>☐ Others: _____</p> <p>☐ None</p> <p>Audit / assessment reports that can be made available upon request:</p> <p>☐ Penetration test</p> <p>☐ TVRA</p> <p>☐ Vulnerability scan</p> <p>☐ Audit reports (e.g., Statement on Standards for Attestation Engagements (SSAE) No. 18, Reporting on Controls at a Service Organisation)</p> <p>☐ Adversarial simulation exercise reports</p>	
2.	Compliance	<p>The following guidelines / standards / regulations are adhered to:</p> <p>☐ Laws governing protection of personal data/information</p> <p>☐ ISO/IEC 27001</p> <p>☐ ISO 9000</p> <p>☐ ISO/IEC 20000</p> <p>☐ CSA Open Certification Framework</p> <p>☐ PCI-DSS</p> <p>☐ Others _____</p>	

3.	Law enforcement and legal disclosure	<p>Law enforcement and legal disclosure practices/policy:</p> <p>_____</p>	
----	--------------------------------------	--	--

Data control

4.	Data ownership	<p>All data on the cloud service is owned by the CSC except for:</p> <p>_____</p> <p>The CSC retains the ownership on the derived data or attributes of cloud usage except for the following:</p> <p>☐ Advertising or marketing</p> <p>☐ Statistical analysis on usage</p> <p>☐ Others: _____</p>	
----	----------------	--	--

5.	Data retention	<p>Data deleted by the CSC is retained as follows:</p> <p>☐ Minimum data retention period: _____</p> <p>☐ Maximum data retention period: _____</p> <p>☐ Deleted immediately</p> <p>Log data retention period:</p> <p>☐ Minimum data retention period: _____</p> <p>☐ Maximum data retention period: _____</p> <p>☐ Not retained</p> <p>CSC data retention period:</p> <p>☐ Minimum data retention period: _____</p> <p>☐ Maximum data retention period: _____</p> <p>☐ Not retained</p>	
----	----------------	--	--

		<p>The following types of data are available for download by the CSC:</p> <p>☐ Log data</p> <p>☐ Others: _____</p>	
--	--	--	--

6.	Data sovereignty	<p>The primary data locations are:</p> <p>☐ Singapore</p> <p>☐ Asia Pacific: _____</p> <p>☐ Europe: _____</p> <p>☐ United States</p> <p>☐ Others: _____</p> <p>The backup data locations are:</p> <p>☐ Singapore</p> <p>☐ Asia Pacific: _____</p> <p>☐ Europe: _____</p> <p>☐ United States</p> <p>☐ Others: _____</p> <p>No. of countries in which data centres operate: _____</p> <p>The CSC's data stored in the cloud environment will never leave the locations specified in item 6:</p> <p>☐ Yes</p> <p>☐ Yes, except as required by law</p> <p>☐ Yes, except as noted: _____</p> <p>☐ No</p>	
----	---------------------	---	--

		<p>CSC's consent is required prior to transferring data to a location not specified in item 6 or a third party:</p> <p>☐ Yes</p> <p>☐ Yes, except as required by law</p> <p>☐ Yes, except as noted: _____</p> <p>☐ No</p> <p><i>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 in storage with cloud service providers.</i></p>	
7.	Non-disclosure	<p>☐ Non-disclosure agreement template can be provided by CSP</p> <p>☐ CSP may use customer's NDA (pending legal review)</p>	
8.	Secure disposal or re-use of resources	<p>How data is securely disposed and how (if any) resources are re-used:</p> <p>_____</p>	
Provider performance			
9.	Availability	<p>The committed network uptime is:</p> <p>☐ _____%</p> <p>☐ Varies according to price plan</p> <p>The committed system uptime is:</p> <p>☐ _____%</p> <p>☐ Varies according to price plan</p> <p>The cloud environment has the following single points of failure:</p> <p>☐ _____</p> <p>☐ None</p>	
10.	Third-party dependency	<p>Areas of critical dependency for service delivery:</p> <p>_____</p>	

11.	BCP / DR	☐ DR protection ☐ Backup and restore service ☐ CSC selectable backup plans ☐ Escrow arrangements ☐ No BCP / DR is available ☐ RPO ☐ RTO ☐ Others, please specify: _____	
12.	Liability	<p>The following terms are available for CSCs if the CSP fails to meet the service commitment:</p> ☐ Network failure Liability: _____ ☐ Infrastructure failure Liability: _____ ☐ VM instance failure Liability: _____ ☐ Migrations Liability: _____ ☐ Unscheduled downtime Liability: _____ ☐ Database failure Liability: _____ ☐ Monitoring failure Liability: _____	

13.	Shared responsibility	☐ Communication of shared roles and responsibilities for which CSC needs to implement and manage for use of this cloud service. URL (or attach file): _____	
Service support			
14.	Change management	The CSP has established the following for changes, migrations, downtime, and other potential interruptions to cloud services: <ul style="list-style-type: none"> ☐ 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. 	
15.	Self-service provisioning and management portal	Provide self-service provisioning and management portal for CSCs to manage cloud services: <ul style="list-style-type: none"> ☐ Yes ☐ No If yes, describe the functions of the self-service provisioning and management portal provided: <ul style="list-style-type: none"> ☐ Allow RBAC ☐ Manage resource pools (e.g., VMs, storage, network) and service templates ☐ Track and manage the lifecycle of each service ☐ Track consumption of services ☐ Health monitoring ☐ Others: _____ 	

16.	Incident and problem management	<p>Delivery mode of support:</p> <p>☐ Access via email</p> <p>☐ Access via portal</p> <p>☐ Access via phone support</p> <p>☐ Direct access to support engineers</p> <p>Availability of support:</p> <p>☐ 24/7</p> <p>☐ Hours of operation during office hours: _____</p> <p>☐ Hours of operation after office hours: _____</p> <p>Service response time: _____</p> <p>Notification time of cloud service outage incidents: _____</p> <p>Communication channel used for notification of cloud service outage incidents: _____</p> <p>The following are available to CSCs upon request:</p> <p>☐ Permanent access to audit records of customer instances</p> <p>☐ Incident management assistance</p> <p>Incident response time: _____</p> <p>Mean time to repair upon detection of faults: _____</p>	
-----	---------------------------------	---	--

17.	Billing	<p>The following billing modes are available (please elaborate granularity of charges and measurement):</p> <p>☐ 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)</p> <p>☐ Fixed pricing: _____ (up to yearly/monthly/daily)</p> <p>☐ Other pricing model: _____</p> <p>☐ Not disclosed</p> <p>☐ Available billing history: _____ months</p>	
18.	Data portability	<p>Importable VM formats: _____</p> <p>Downloadable formats: JSON/XML/other open formats (to specify) _____</p> <p>Supported operating systems: _____</p> <p>Language versions of supported operating systems: _____</p> <p>Supported database formats: _____</p> <p>Policy/guide available: _____</p> <p>API:</p> <p>☐ Common</p> <p>☐ Customised</p> <p>Upon service termination or prolonged outage, data is available through:</p> <p>☐ Physical media</p> <p>☐ Standard methods as described above</p> <p>☐ Other methods: _____</p>	

19.	Interoperability	<p>Use of industry standards and availability of APIs to support interoperability:</p> <p>☐ Transport supported (e.g., REST based HTTPS/MQTT): _____</p> <p>☐ Format supported (e.g., JSON/XML): _____</p> <p>☐ APIs supported: _____</p> <p>☐ Other methods: _____</p> <p>_____</p> <p>Guide available: _____</p>	
20.	Access	<p>Type of access to the service is through:</p> <p>☐ Public access</p> <p>☐ Private access (e.g., VPN, dedicated link)</p> <p>☐ IPv6 access is supported</p> <p>☐ Other access methods: _____</p> <p>_____</p> <p>_____</p> <p>Public access speed (shared bandwidth) in Mbps: _____</p>	
21.	User management	<p>☐ Identity management</p> <p>☐ RBAC</p> <p>☐ Federated access model</p> <p>☐ Integration with Identity management solutions</p> <p>☐ Others: _____</p>	
22.	Lifecycle	<p>The CSC may select the following for service upgrades and changes:</p> <p>☐ Automatic provisioning</p> <p>☐ CSC customisable provisioning</p>	

Security configurations			
23.	Security configuration enforcement checks	<p>Security configuration enforcement checks are performed:</p> <p>☐ Manually</p> <p>☐ Using automated tools</p> <p>How often are enforcement checks being performed to ensure all security configurations are applied?</p> <p>_____</p>	
24.	Multi-tenancy	<p>☐ Distinct physical hosts</p> <p>☐ Distinct physical network infrastructure</p> <p>☐ Virtual instance grouping</p> <p>☐ Cloud service customer definable security domains</p> <p>☐ Cloud service customer customisable firewall</p> <p>☐ Cloud service customer definable access policies</p>	
25.	Hybrid cloud provision	<p>Ability to monitor, track, apply and enforce CSC's security and privacy policies on its cloud workloads:</p> <p>☐ Data protection and encryption, key management enforcement, geolocation-based/resource pools and secure migration of cloud workloads</p> <p>☐ Key management and keystore controlled by CSC</p> <p>☐ Persistent data flow segmentation before and after geolocation-based/resource pools secure migration</p> <p>☐ Compliance enforcement for regulated workloads between on-premises private and hybrid/public cloud</p> <p>☐ Others: _____</p>	

Service elasticity			
26.	Capacity elasticity	<p>The following capacity elasticity options are available:</p> <ul style="list-style-type: none"> ☐ 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) 	
27.	Network resiliency and elasticity	<p>The following network resiliency and elasticity options are available:</p> <ul style="list-style-type: none"> ☐ 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: ____	
28.	Storage redundancy and elasticity	<p>The following storage redundancy and elasticity options are available:</p> ☐ 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 (please specify): _____ ☐ Minimum storage I/O performance during peak periods: _____ ☐ Minimum period to scale up storage I/O throughput: _____	

Software supply chain security											
29.	Vendor software assurance	<p>Describe the process used to assess the software development and quality assurance practices of third-party software vendors, particularly to ensure the security of any sensitive data they may access.</p> <hr/> <hr/> <hr/>									
30.	Source code escrow	<p>List critical software acquired from third-party vendors and indicate if a source code escrow arrangement is in place.</p> <table border="0"> <thead> <tr> <th>Software description</th> <th>Source code escrow</th> </tr> </thead> <tbody> <tr> <td><hr/></td> <td>☐ Yes ☐ No</td> </tr> <tr> <td><hr/></td> <td>☐ Yes ☐ No</td> </tr> <tr> <td><hr/></td> <td>☐ Yes ☐ No</td> </tr> </tbody> </table> <p>If source code escrow is not used, describe the alternative strategies used to mitigate vendor viability risk.</p> <hr/> <hr/>	Software description	Source code escrow	<hr/>	☐ Yes ☐ No	<hr/>	☐ Yes ☐ No	<hr/>	☐ Yes ☐ No	
Software description	Source code escrow										
<hr/>	☐ Yes ☐ No										
<hr/>	☐ Yes ☐ No										
<hr/>	☐ Yes ☐ No										