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, the public Cloud Service Provider shall indicate accordingly with remarks

Cloud Service Provider Contact Information

Company name	:	NEC ASIA PACIFIC PTE LTD
Primary address	:	80 Bendemeer Road #05-01/02 Hyflux Innovation Centre, Singapore 339949
Web address	:	http://sg.nec.com/
Contact name	:	Edi Helmy
Contact number	:	6782 5919
MTCS certificate number	:	_____

Company Stamp :   Signature of company representative :

Certification Body Contact Information

Company name	:	TUV SUD PSB Pte Ltd
Primary address	:	No. 1 Science Park Drive, Singapore 118221.

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

Company Stamp   Signature of company representative : Catherine Teh

Annex A

(normative)

Cloud service provider disclosure

Cloud Service Provider Background

Overview of service offering:

Infrastruture as a Service (IAAS)

Service model:

☒ Virtual machine instances owned by the user

☒ 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 user has the right to audit: ☒ Virtual machine instances owned by the user ☒ Network facilities ☒ Compliance with applicable standard ☒ Technical controls ☒ Policies and governance ☒ Data centre facilities ☐ Others: _____ ☐ None Regulators recognized by Singapore law have the right to audit: ☒ Virtual machine instances owned by the user ☒ Network facilities	NIL

Annex A

(normative)

Cloud service provider disclosure

<table>
<tr><td></td><td></td><td>

☒ Compliance with applicable standard

☒ 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 engagement (SSAE) No. 16, Reporting on Controls at a Service Organisation)

</td><td></td></tr>
<tr><td>2.</td><td>**Compliance**</td><td>

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: <u>ANSI/TIA-942:2014, SAP EBM</u>

</td><td>_____</td></tr>
<tr><td>3.</td><td>**Data ownership**</td><td>

All data on the cloud service is owned by the cloud user except for: _____

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: _____

</td><td>_____</td></tr>
<tr><td>4.</td><td>**Data retention**</td><td>Data deleted by the user is retained as follow</td><td>_____</td></tr>
</table>

Annex A

(normative)

Cloud service provider disclosure

<table>
<tr>
<td></td>
<td></td>
<td>
☒ Minimum data retention period is <u>7 days</u>
☒ Maximum data retention period is <u>7 years</u>
☐ Deleted immediately

Log data is retained for a period of:
☒ Minimum data retention period as follows <u>3 months</u>
☒ Maximum data retention period is <u>1 year</u>
☐ Not retained

User data is retained for a period of:
☒ Minimum data retention period is <u>7 days</u>
☒ Maximum data retention period is <u>7 years</u>
☐ Not retained

The following types of data are available for download by the cloud user:
☐ Log data
☐ Others _____
</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>**Data sovereignty**</td>
<td>
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: <u>1</u>

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: <u>Overseas customer data</u>
</td>
<td>_____</td>
</tr>
</table>

Cloud service provider disclosure

		☐ 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: _____ ☐ No **Note:** *Cloud users are responsible for determining the impact of data protection and data sovereignty laws on the location where data is stored. In addition, users should understand the risk 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 user customer's NDA (pending legal review)	_____
Provider Performance			
7.	Availability	The committed network uptime is: ☒ 99.9 % ☐ Varies according to price plan The committed system uptime is: ☒ 99.9 % ☐ 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 ☐ RPO _____	_____

Cloud service provider disclosure

		☐ RTO _____ ☐ 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: based on SLA terms ☒ Infrastructure failure Liability: based on SLA terms ☒ Virtual machine instance failure Liability: based on SLA terms ☐ Migrations Liability: _____ ☒ Unscheduled downtime Liability: based on SLA terms ☐ Database failure Liability: _____ ☒ Monitoring failure Liability: based on SLA terms	——
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	——

Cloud service provider disclosure

		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: <u>0900 - 1800</u> ☒ After office hours support, please specify the hours of operations: <u>1800 - 0900</u> ☒ Service response time: <u>4hrs (Standard)</u> The following are available to users upon request: ☐ 24 x 7 ☐ Permanent access to audit records of customer instances ☒ Incident management assistance Incident response time: <u>4 hours (Standard)</u> 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/yuear for SaaS) ☒ Fixed pricing <u>monthly</u> (up to yearly/monthly/daily) ☒ Other pricing model <u>One-Time Charges</u>	——

Cloud service provider disclosure

		☐ Not disclosed	———
		☐ Available billing history: _____ Months	
14.	Data portability	Importable VM formats: <u>VMDK</u> Downloadable formats: _____ Supported operating systems: <u>Windows, Linux</u> Language versions of support operating systems: <u>English</u> Supported database formats: <u>SQL, Oracle</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>20mbps</u>	———
16.	User management	☒ Identity management ☒ Role based access control ☐ Federated access model ☐ Integration with identity management solutions ☐ Other _____	———
17.	Lifecycle	The cloud user may select the following for service upgrades and changes: ☐ Automatic provisioning ☒ User customisable provisioning	———
Security Configurations			

Annex A

(normative)

Cloud service provider disclosure

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? _____	_____
19.	**Multi-tenancy**	☐ Distinct physical hosts ☐ Distinct physical network infrastructure ☒ Virtual instance grouping ☐ Using automated tools	_____
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 p computing resources _____ ☐ Minimum additional capacity guaranteed per account _____ (number of cores of 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 100 Mbps ☐ Maximum usable IPs _____ ☐ Load balancing ports _____ ☐ Load balancing protocols _____ ☒ Anti-DDOS protection systems or services ☐ Defence-in-depth mechanisms, please specify: _____	_____

(normative)

Cloud service provider disclosure

		☐ Network traffic isolation, please specify: ___ ☒ Shared or dedicated bandwidth, please specify: <u>Either</u> ☒ 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: <u>based on subscription</u> ☒ Maximum storage capacity for single user, please specify: based on subscription ☒ Maximum expandable storage, please specify: <u>based on subscription</u> 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 ___	___